Immigration, Refugees   Immigration, Réfugiés
and Citizenship Canada   et Citoyenneté Canada
Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

Top Priority Projects Underway at A2SC

Project prioritization criteria: Support Immigration levels, increase efficiencies, and/or enhance program integrity.
With current resources, AA team can undertake between 5 and 7 projects concurrently.
The estimated delivery dates hinge on many dependencies, including:

- Availability of experts within Ops to adapt business processes and ensure governance.
- IT support
- Addressing applicable Legal, Privacy, Policy and Governance considerations

Update: July 7, 2021

Project	Lead Branch	Description	Outcome sought	Status/Approach	Estimated Delivery	Potential Benefits / Impact
TRV triage	IN, CN	• Update the existing China/India models and incorporate enhancements to deal with COVID-19 realities. • Expand to all other countries.	Accelerate processing, reduce inventory, free up officers, and improve preparedness for travel resumption.	• In-Canada: triage tool is ready. Awaiting legal opinion. • China: model is ready. Consulting Legal on rules. • India: model almost finished. Need networks to check "false positives" to assess accuracy of the model. • Rest of world: barely started. • All models need to be updated to the new TR eApp, otherwise they will eventually malfunction. • Need networks to assess the impact of the aging inventory (e.g. expired passports) on processing speed to assess if models will yield expected efficiencies	Clients in Canada: mid-July 2021 China / India: End of July 2021 Global Expansion: end of August 2021	Green bin expectations: • China: 20-25% • India: 5-15% • Rest of world: unknown
Mexico Mailbox Triage	IN	Automate the manual triage using AA tools using text mining, and machine learning. IRCC Mexico processes PRs from 48 countries and TRs from 15 countries. The emails are a huge operational pressure.	Reduce the Operational Pressure and Accelerate processing	• Tool is ready. • Waiting for GAC to enable automatic forwarding of emails from the Mexico inbox to our cloud account. • The solution should be operational 1-2 weeks after GAC approves.	Mid to end of July 2021	Increased productivity and accuracy of triage (not quantified)
Work Permit extensions - Phase 2	CN	Extend the pilot for PGWP that was launched in March 2021 to all other WP-extensions. The PGWP pilot yielded efficiency gains of 21%	Accelerate processing and reduce inventory	• Tool is ready. • CN is currently very busy with PGWP intake which has surged since the end of the spring semester. This will push back the launch.	Aug 1, 2021	Hopefully will match the 20% efficiency gains observed for PGWP
Lighthouse for SP	IN, IRM	Identify high-risk files for verifications, building on July 2020 pilot. Because this pilot focuses on improving integrity, it is not expected that processing times will change.	Improve integrity, increase effectiveness of verifications	• Undergoing a last update of the rules with Legal / Privacy prior to launch	Aug 1, 2021	Increased integrity and fraud detection
TR to PR pathway	Solutions Team, CN	Extend the WP-EXT triage approach to the TR to PR caseload. That approach yielded efficiency gains of 21% for PGWP	Accelerate processing and support levels achievement	• Tool is almost ready • Awaiting legal opinion	End of August 2021	Hopefully will match the 20% efficiency gains observed for PGWP
CEC	Solutions Team, CN	Identify low-risk files in the inventory for instant eligibility approval	Accelerate processing and support levels achievement	Still analyzing the data to determine if it's feasible to create sufficiently strong rules to automate eligibility approvals	End of August 2021	Size of green bin it still unknown
PNP	Solutions Team, CN???	Identify low-risk files in the inventory for instant eligibility approval	Accelerate processing and support levels achievement	Still analyzing the data to determine if it's feasible to create sufficiently strong rules to automate eligibility approvals	End of August 2021	Size of green bin it still unknown
FC Spousal – Overseas Phase 2	IN, Beijing	Use OCR to extract text from supporting documents to improve triage and identify low-risk files for automated approval	Accelerate processing and support levels achievement	• Initial results are promising but the progress is slowed down by other priorities. • Working with the Journey Lab and IT to automate the process for uploading supporting documents to the cloud.	TBD	Size of green bin it still unknown

Issue 587564 - Access to a sub-folder in the SPSS server repository

Assigned To: Kaur.Harpreet

State: Closed

Created Date: 05/28/2020 2:28 PM

Description:

Could we please ensure that the following persons have full access rights to the folder   in the new   repository?
Thanks!

- Ahmad.Imran
- Haffaf.Amine
- Son.David
- Tipenko.Elena
- Van.My-Phuong
- Haymes.Michael

History

05/28/2020 3:05 PM Nhan.Phuong:
Harpreet, would you please look into this access in   Thank you

05/29/2020 1:58 PM Podeanu.Robert:
Closing ticket

A3489879_1-000002

s.16(2)(c)

Issue 613065 - Netezza Access - Bruno Afonso

Assigned To: Lambier.Mark

State: Closed

Created Date: 09/10/2020 10:54 AM

Description:

Could you please give Bruno the same access that Michael Haymes has in the   Bruno is a new A2SC Data Scientist who will work with Mike and other Data Scientists on Watchtower.

History

09/10/2020 3:09 PM Lambier.Mark:
DONE..

Bruno's Access:

Michael's Access:

s.16(2)(c)

User Properties   ✕

MICHAEL.HAYMES
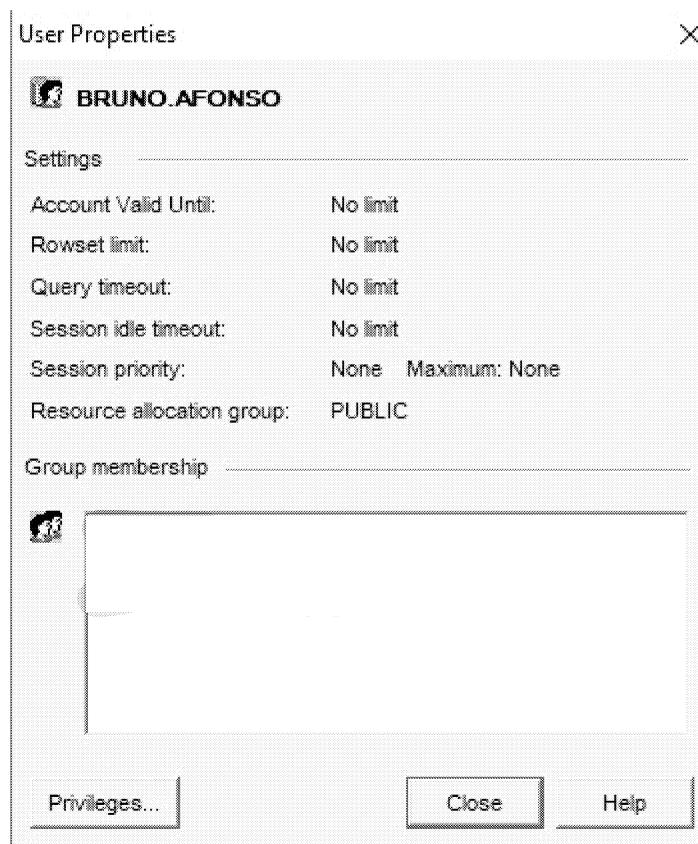
Settings

Account Valid Until:	No limit
Rowset limit:	No limit
Query timeout:	No limit
Session idle timeout:	No limit
Session priority:	None Maximum: None
Resource allocation group:	PUBLIC

Group membership

Privileges...   Close   Help

09/10/2020 3:22 PM Rizvi.Haider:
Client has been notified. Closing ticket.

Bug 724864 - CLIENT: accessibility issues on Personal Info page (paper)

Assigned To: Dupuis.Marcel

State: Closed

Created Date: 10/12/2021 10:27 AM

Description:

According to "WAVE® Web Accessibility Evaluation Tool" (Chrome extension), on the "Provide your personal information" page, there's two WCAG accessibility issues on "UCI" and "Application Number" fields
error: Missing form label
see screenshot "missing-labels.png"

Test using Wave and Lighthouse for accessibility issues.

History

10/29/2021 5:19 AM Siddiqi.Zahid:
@Leclerc.Eric Are there similar issues on the upload more documents page?

10/29/2021 7:12 AM Leclerc.Eric:
@Siddiqi.Zahid   no other accessibility were found on paper app at the time of testing

11/03/2021 9:26 AM Leclerc.Eric:
a new issue was discovered by Marcel yesterday, a new story/bug was created as it's a different a11y issue on a different page. ref: Bug 731860: CLIENT: accessibility issues on Upload Documents page (paper)

s.16(2)(c)

Overview of Watchtower (WT) Risks and Mitigations

Risk	

Pages 7 to / à 26

are withheld pursuant to sections

sont retenues en vertu des articles

16(1)(b), 16(1)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Page 27

is withheld pursuant to sections

est retenue en vertu des articles

16(1)(b), 16(1)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Pages 28 to / à 30

are withheld pursuant to sections

sont retenues en vertu des articles

16(1)(b), 16(1)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Pages 31 to / à 39

are withheld pursuant to sections

sont retenues en vertu des articles

16(1)(b), 16(1)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Government   Gouvernement
of Canada   du Canada

Algorithmic Impact Assessment

Algorithmic Impact Assessment Results

Save   Choose File No file chosen   Start Again   Link to GitHub project repository

---

> ⓘ Information in the AIA is only stored locally on your computer, and the Government of Canada does not have access to the information you place into the tool. If you wish to keep your work, please save the data locally for future use.

On this page

- Impact Level
- Requirements Specific to Impact Level:
- Mitigation Measures
- Questions and Answers
  - Project Details
  - Impact Questions and Answers
  - Mitigation Questions and Answers

> ⓘ Impact Level: 2   Current Score: 35   Raw Impact Score: 35   Mitigation Score: 25

Requirements Specific to Impact Level: 2

Peer Review

At least one of: Qualified expert from a federal, provincial,territorial or municipal government institution Qualified members of faculty of a post - secondary institution Qualified researchers from a relevant non - governmental organization Contracted third - party vendor with a related specialization Publishing specifications of the Automated Decision System in a peer - reviewed journal A data and automation advisory board specified by Treasury Board Secretariat

Notice

Plain language notice posted on the program or service website.

Human-in-the-loop for decisions

Decisions may be rendered without direct human involvement.

Explanation Requirement

In addition to any applicable legislative requirement, ensuring that a meaningful explanation is provided upon request for any decision that resulted in the denial of a benefit, a service, or other regulatory action.

Testing

A3745411_1-000040

Before going into production, develop the appropriate processes to ensure that training data is tested for unintended data biases and other factors that may unfairly impact the outcomes. Ensure that data being used by the Automated Decision System is routinely tested to ensure that it is still relevant, accurate, and up-to-date.

Monitoring

Monitor the outcomes of Automated Decision Systems on an ongoing basis to safeguard against unintentional outcomes and to ensure compliance with institutional and program legislation, as well as this Directive.

Training

Documentation on the design and functionality of the system.

Contingency Planning

None

Approval for the system to operate

None

Link to the Directive on Automated Decision-Making Impact Level Requirements

Mitigation Measures

The following internal stakeholders have been consulted:

A documented process is currently in place to test datasets against biases and other unexpected outcomes.

Accountabilities for the design, development, maintenance, and improvements for the system have been assigned.

The audit trail clearly identifies the authority or delegated authority as identified in legislation.

The system records all the recommendations or decisions made by the system.

All key decision points are identifiable in the audit trail.

All key decisions points are linked to the relevant legislation, policy or procedure.

The system's audit trail indicates all of the decision points made by the system.

The system's audit trail can be used to help generate a notification of the decision (including a statement of reasons or other notifications) where required.

The audit trail identifies which version of the system was used for each decision.

The system's audit trail shows who the authorized decision-makers are.

The system is able to produce reasons for its decision or recommendations when required.

There is a process in place to grant, monitor, and revoke access permission to the system.

There is a mechanism to capture feedback by users of the systems.

A3745411_2-000041

There is a recourse process in place for clients that wish to challenge the decision.

The system enables human override of system decisions.

There is a process in place to log instances when overrides were performed.

Questions and Answers

Project Details

Name of Respondent

English Content :

Steven Gonzalez

French Content :

Job Title

English Content :

Assistant Director

French Content :

Department

Citizenship and Immigration (Department of)

Branch

English Content :

OPPB

French Content :

Project Title

English Content :

Watchtower pilot

French Content :

Project Phase   **Points:** 0

Implementation

Please provide a project description:

English Content :

AIA for administrative pilot of Watchtower on TR lines of business

French Content :

A3745411_3-000042

What is motivating your team to introduce automation into this decision-making process? (Check all that apply)

- Improve overall quality of decisions
- The system is performing tasks that humans could not accomplish in a reasonable period of time
- Use innovative approaches

Please check which of the following capabilities apply to your system.

- Text and speech analysis: Analyzing large data sets to recognize, process, and tag text, speech, voice, and make recommendations based on the tagging
- Risk assessment: Analyzing very large data sets to identify patterns and recommend courses of action and in some cases trigger specific actions
- Content generation: Analyzing large data sets to categorize, process, triage, personalize, and serve specific content for specific contexts

Impact Questions and Answers

Is the project within an area of intense public scrutiny (e.g. because of privacy concerns) and/or frequent litigation?	**Points:** +3
Yes	
Are clients in this line of business particularly vulnerable?	**Points:** +0
No	
Are stakes of the decisions very high?	**Points:** +0
No	
Will this project have major impacts on staff, either in terms of their numbers or their roles?	**Points:** +0
No	
Will you require new policy authority for this project?	**Points:** +0
No	
The algorithm used will be a (trade) secret	**Points:** +0
No	
The algorithmic process will be difficult to interpret or to explain	**Points:** +0
No	

Does the decision pertain to any of the categories below (check all that apply):

• Economic interests (grants and contributions, tax benefits, debt collection)	**Points:** +1
• Access and mobility (security clearances, border crossings)	**Points:** +1
Will the system only be used to assist a decision-maker?	**Points:** +1
Yes	
Will the system be replacing a decision that would otherwise be made by a human?	**Points:** +0
No	
Will the system be replacing human decisions that require judgement or discretion?	**Points:** +0
No	

A3745411_4-000043

Is the system used by a different part of the organization than the ones who developed it?   **Points:** +4

Yes

Are the impacts resulting from the decision reversible?   **Points:** +2

Likely reversible

How long will impacts from the decision last?   **Points:** +2

Some impacts may last a matter of months, but some lingering impacts may last longer

Please describe why the impacts resulting from the decision are as per selected option above.

English Content :

Impacts are highest for SP and WP, where a client could miss a semester or a worker could miss a job opportunity. Impacts for TRV are lower. TRV far outnumber SP and WP combined.

French Content :

The impacts that the decision will have on the rights or freedoms of individuals will likely be: **Points:** +1

Little to no impact

Please describe why the impacts resulting from the decision are (as per selected option above).

English Content :

Foreign nationals do not possess a "right" to enter Canada. Impacts are better framed in terms of economic interests (see below) rather than "rights or freedoms."

French Content :

The impacts that the decision will have on the health and well-being of individuals will likely be: **Points:** +1

Little to no impact

Please describe why the impacts resulting from the decision are (as per selected option above)

English Content :

TR lines of business are generally not related to health of clients. It is rare that a client is seeking medical attention in Canada.

French Content :

The impacts that the decision will have on the economic interests of individuals will likely be: **Points:** +2

Moderate impact

Please describe why the impacts resulting from the decision are (as per selected option above)

A3745411_5-000044

English Content :

Missing a semester or a job opportunity could affect the financial situation of the client. But these cases are fewer in number than TRVs, where the impact on economic interests of the client is generally low.

French Content :

The impacts that the decision will have on the ongoing sustainability of an environmental ecosystem, will likely be: **Points:** +1

Little to no impact

Please describe why the impacts resulting from the decision are (as per selected option above)

English Content :

Not related to the environment

French Content :

Will the Automated Decision System use personal information as input data? **Points:** +4

Yes

What is the highest security classification of the input data used by the system? (Select one) **Points:** +3

Protected B / Protected C

Who controls the data? **Points:** +1

Federal government

Will the system use data from multiple different sources? **Points:** +0

No

Will the system require input data from an Internet- or telephony-connected device? (e.g. Internet of Things, sensor) **Points:** +0

No

Will the system interface with other IT systems? **Points:** +4

Yes

Who collected the data used for training the system? **Points:** +1

Your institution

Who collected the input data used by the system? **Points:** +1

Your institution

Will the system require the analysis of unstructured data to render a recommendation or a decision? **Points:** 0

Yes

What types of unstructured data? (Check all that apply)

- Audio and text files **Points:** +2

Mitigation Questions and Answers

Internal Stakeholders (Strategic policy and planning, Data Governance, Program Policy, etc.) **Points:** +1

A3745411_6-000045

Yes

External Stakeholders (Civil Society, Academia, Industry, etc.)   **Points:** +0

No

Do you have documented processes in place to test datasets against biases   **Points:** +2
and other unexpected outcomes? This could include experience in applying
frameworks, methods, guidelines or other assessment tools.

Yes

Is this information publicly available?   **Points:** +0

No

Have you developed a process to document how data quality issues were   **Points:** +0
resolved during the design process?

No

Is this information publicly available?   **Points:** +0

No

Have you undertaken a Gender Based Analysis Plus of the data?   **Points:** +0

No

Is this information publicly available?   **Points:** +0

No

Have you assigned accountability in your institution for the design,   **Points:** +2
development, maintenance, and improvement of the system?

Yes

Do you have a documented process to manage the risk that outdated or   **Points:** +0
unreliable data is used to make an automated decision?

No

Is this information publicly available?   **Points:** +0

No

Is the data used for this system posted on the Open Government Portal?   **Points:** +0

No

Does the audit trail identify the authority or delegated authority identified   **Points:** +1
in legislation?

Yes

Does the system provide an audit trail that records all the recommendations   **Points:** +2
or decisions made by the system?

Yes

Are all key decision points identifiable in audit trail?   **Points:** +2

Yes

Are all key decision points within the automated system's logic linked to the   **Points:** +1
relevant legislation, policy or procedures?

Yes

Do you maintain a current and up to date log detailing all of the changes   **Points:** +0
made to the model and the system?

No

Does the system's audit trail indicate all of decision points made by the   **Points:** +1
system?

Yes

Can the audit trail generated by the system be used to help generate a notification of the decision (including a statement of reasons or other notifications) where required?

Points: +1

Yes

Does the audit trail identify precisely which version of the system was used for each decision it supports?

Points: +2

Yes

Does the audit trail show who an authorized decision-maker is?

Points: +1

Yes

Is the system able to produce reasons for its decisions or recommendations when required?

Points: +2

Yes

Is there a process in place to grant, monitor, and revoke access permission to the system?

Points: +1

Yes

Is there a mechanism to capture feedback by users of the system?

Points: +1

Yes

Is there a recourse process established for clients that wish to challenge the decision?

Points: +2

Yes

Does the system enable human override of system decisions?

Points: +2

Yes

Is there a process in place to log the instances when overrides were performed?

Points: +1

Yes

Does the system's audit trail include change control processes to record modifications to the system's operation or performance?

Points: +0

No

Have you prepared a concept case to the Government of Canada Enterprise Architecture Review Board?

Points: +0

No

Have you completed a Privacy Impact Assessment or revised an existing one?

Points: +0

No

Does your system reflect Privacy by Design principles?

Points: +0

No

Export

Export English Document   Export French Document

▶ English Content

▶ French Content

Date modified: 2020-06-03

A3745411_8-000047

Version: 0.8.1

A3745411_9-000048

Immigration, Refugees   Immigration, Réfugiés
and Citizenship Canada   et Citoyenneté Canada
Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

Immigration, Refugees   Immigration, Réfugiés
and Citizenship Canada   et Citoyenneté Canada

Director General   Directeur général
Integrity Risk   Orientation sur les
Management   risques pour l'intégrité

Ottawa K1A 1L1

F- 07790719

PROTECTED B

MEMORANDUM TO THE DIRECTOR GENERAL, OPERATIONAL PLANNING AND PERFORMANCE BRANCH AND THE DIRECTOR GENERAL, INTEGRITY RISK MANAGEMENT BRANCH

GOVERNANCE AND BUSINESS OWNERSHIP OF LIGHTHOUSE TOOL

FOR APPROVAL

SUMMARY
• This memorandum seeks your approval of the Lighthouse Governance Framework ('the Framework') to ensure agreement on shared ownership and responsibility.   • The Framework provides oversight on the management of the Lighthouse tool and outlines accountabilities, roles, and responsibilities for its development, implementation and use. Business ownership of Lighthouse will be shared between the Operational Planning and Performance Branch (OPPB) and Integrity Risk Management Branch (IRM).   • Lighthouse is an AI-based risk indicator solution that has been developed to automatically and comprehensively extract risk and fraud patterns from source data from the Global Case Management System for any applicable line of business. The tool does not involve automated decision-making.   • We recommend that you approve the Lighthouse Governance Framework and its business co-ownership by signing the approval page within the Framework as well signing this memorandum by August 18, 2021.

BACKGROUND:

• In recent years, the demand for artificial intelligence (AI) solutions to assist with the Department's program delivery has been steadily increasing, primarily to address challenges in volume management. In April 2020, the Treasury Board Secretariat's *Directive on Automated Decision-Making* came into force to outline high-level requirements for automated solutions in the Government of Canada. In June 2019, IRCC also developed its own internal *Policy Playbook* on Automated Support for Decision-Making.

Canada

A3745412_1-000049

PROTECTED B

- Formerly known as Watchtower, Lighthouse is an AI-based risk indicator solution that has been developed to automatically and comprehensively extract risk and fraud patterns from source data from the Global Case Management System for any applicable line of business. It is a data-mining tool that identifies and presents fact-based information. The tool's findings can be configured to produce customized reports to satisfy various needs for Risk Assessment Units within the integrated processing network, allowing them to direct their resources to potential cases of concern. This will assist Risk Assessment Units with investigations and large-scale trend analysis, and lead to efficiencies in the identification and processing of higher-risk cases.

- Lighthouse does not make recommendations or render administrative decisions about clients or their applications. Since all eligibility and admissibility decisions will be made by decision makers and the tool would not be involved in making any decisions, an Officer of Record would not be required to act as the authority under the Instrument of Designation and Delegation. Measures have been taken to ensure that human intervention is part of every stage of the tool's application.

- In its initial pilot, which ran in summer 2020 on the caseload of global study permit applications, Lighthouse uncovered over 800 unique risk patterns, some of which led to identification of larger-scale fraud trends. By using the tool's full potential and focusing our risk management efforts where attention is needed most, the Operations Sector can potentially create processing efficiencies in cohorts that do not require as much effort.

- A governance framework (in annex) has been drafted to set priorities for Lighthouse's use, explain its processes, outline related roles and responsibilities, and ensure transparency in the usage of the tool.

CURRENT STATUS:

- Each usage of the tool that involves live applications requires a dedicated project charter to complement the Framework by addressing the specifics of the usage in question. By having a broader framework, the general principles of the tool on its usage and governance can be agreed upon in advance which, when supplemented by specific project charters, would facilitate procedures and expedite implementations.

- Business ownership of Lighthouse will be shared between OPPB and IRM, given each branch's mandate and the potentially broad scope of the Lighthouse project. The responsibility of development, implementation and maintenance of the tool will lie with the Advanced Analytics Solutions Centre team within OPPB. The team will focus on the tool's technical design and record-keeping as it relates to the design and configuration data of the tool, ensuring that the privacy and legal requirements and recommendations are followed. IRM will be responsible for operationalizing the program-level aspects of the tool's findings as well as maintaining administrative aspects of the tool, such as quality management and ensuring the governance framework remains evergreen. IRM will also lead working group meetings to bring forward any necessary changes, in order to respond to departmental priorities or changing risk management practices and develop a consistent approach for the department.

PROTECTED B

- CDO will play a key role in overseeing the tool's data management. CDO will seek approval on data inputs specific to each implementation or pilot from the Data Executive Steering Committee (DESC), who will in turn inform Issues Management Committee (IMC).

- The processing networks (IN, CN, and DN) and their Risk Assessment Units will operationalize case specific aspects of the tool's findings, and work with IRM and OPPB to map out operational processes and to improve its effectiveness and usage. Case Management Branch will assess larger-scale fraud trends flagged by the tool and ensure resulting business intelligence is shared with all other stakeholders.

- Strategic and Program Policy Branch will be responsible for providing guidance on policies, including Algorithmic Impact Assessments, and for coordinating engagement with other stakeholders and the public.

- Stakeholders such as Migration Health Branch, Citizenship and Passport Programs Branch, and Transformation and Digital Solution Sector (TDSS) may participate in Lighthouse working groups in the future, should the tool's involvement become relevant to their respective mandates.

- This division of roles reflects the approach presented to the Issues Management Committee in December 2018, and aligns with the 2018-2023 Operations Sector Strategic Plan.

CONSULTATIONS:

- The Framework has been developed in close collaboration with key partners. Approval was obtained at the Director level from Operations Planning and Performance Branch, Integrity Risk Management Branch, Centralized Network, International Network, Domestic Network, Immigration Program Guidance Branch, ATIP Division, Legal Services Unit, Strategic Policy and Planning Branch, Case Management Branch, Admissibility Branch, Internal Audit and Accountability Branch, and Chief Data Officer.

RECOMMENDATION(S):

- We recommend that you approve the Framework and its business co-ownership by signing the approval page within the Framework document as well as in this memorandum.

NEXT STEP(S):

- Following your approval, the Framework will be applied to the operational environment starting in fall 2021.

- The second global study permit pilot, which was initially scheduled to run from March to September 2021, is currently in its early consultation phase. Representatives from IRM, OPPB,

PROTECTED B

CN, DN, and IN are meeting weekly, reviewing patterns mined by the tool, and agreeing on procedures.

e-approved
Elizabeth Stronach
Director, Integrity Risk Management Branch

e-approved
Steven Gonzalez
Director, Operational Planning and Performance Branch

DG Signature
Alain Desruisseaux
Director General, Integrity Risk Management Branch

☐ I concur
☐ I do not concur

DG Signature
Marie-Josee Dorion
Director General, Operational Planning and Performance Branch

☐ I concur
☐ I do not concur

Annex: Governance Framework for Lighthouse

Pages 53 to / à 56

are withheld pursuant to sections

sont retenues en vertu des articles

16(1)(b), 16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Integrated Networks Steering Committee

Record of Decision
May 13, 2021

Record of Discussion	Presenter(s)
Chair Opening Remarks/Approval of Record of Discussion	**OPPB/IN**
Please send comments by Friday COB or the RoD will be considered approved.	
Admissions Preparation	**OPP**
Business Resumption – NIL	
Integrated Network-	
Lighthouse SP Pilot	**OPP**

Objectif: To seek committee endorsement to begin the pilot to test the use of the tool in improving program integrity and fraud detection efficiency in the global SP caseload. OPP is also seeking a decision regarding the ownership of the program

Documents:

Watchtower   LH_INSC_QnATalking
Integrated Network St   Points.docx

Roundtable:
- IN confirmed their support for this pilot and moving forward to the Data Steering Committee. IN would like to have lighthouse brought back to INSC for endorsement of future phases.
- IN is interested in assisting OPP's Advanced Analytics team in moving toward more consistent reporting on trends, ground intelligence and external information to identify risks for this tool so ·

- IRM offered support for this pilot
- CN gave support for this pilot and IN's proposal to include external data where possible. CN requesting to add building a communications plan and meeting with the bargaining agents to the next steps
- IPG is fully supportive of the pilot and tool. They too support IN's suggestion to build upon the tool with   in order to strengthen program integrity.
- OPP supports the idea of incorporating external factors/trends in order to rely less upon self-declared information
- In terms of ownership, OPP notes that an Officer of Record Memo would not be required for this scenario given the tool does not make decisions, but we need someone to greenlight the pilot.

Decision: The table endorses moving forward with the lighthouse SP Pilot

Next steps:
- OPP to bring this item forward to the Data Executive Steering Committee scheduled for late May
- To determine the business owner and ensure clear accountabilities
- OPP to brief management teams and bargaining agents

	IPG

Canada
A3745416_1-000057

Final Round Table
IPG:
• IPG to schedule a meeting with network DGs to ensure clear and consistent approach to processing TR and PR for India/Pakistan
OPP Update on CEC Rounds:
• There continue to be concerns around CRS scores; therefore, a smaller round will be conducted this week than originally planned. Instead of the 6,000 round we will be doing roughly 4200. This will be reviewed on a weekly basis until our inventory with CRS scores over 400 replenishes
• To note this could mean the next 12 rounds could be lower than anticipated making it more difficult to reach targets
• This discussion will be brought to the next LPPC

Members	Branch	In Attendance	Replacement
CO-Chairs			
Blair Haddock	OPPB	Yes	
Pemi Gill	IN	Yes	
Attendance			
Isabelle Daoust	CMB	Yes	
Andre Baril	IPG	Yes	
Sylvain Beauchamp	CEB	No	Cynthia Rebaza
Peter Mielke	OPPB - DART	Yes	
Alain Desruisseaux	IRM	Yes	
Craig Shankar	MHB	Yes	
Tara Davidson	CN	Yes	
Alexandra Hiles	DN	Yes	
Maxine Ifill	CPP	Yes	
Sean McNair	IDI	Yes	
Jean-Marc Gionet	RASO	Yes	
Brittany Doyle	Secretariat	Yes	

Observers	Branch
Christopher Kerr	ST
Julia Gurr-Lacasse	IN
Martin Barry	IPG
Kevin Terry	IN
Malcolm Eales	IPG
Melanie Mercier	IPG
Elizabeth Snow	IN
RoseAnne Poirier	CN
Marie-Josee Dorion	CPP
Steven Gonzalez	OPPB

2

Ellie Weber	CN
Philippe Desrochers	CMB
Marie-Josee Dorion	ST
Tanya Knight	IRM
Ania Delisle	OPPB
Benjamin Bigio	IPG

3

A3745416_3-000059

Lighthouse Risk Identification System

June 2021
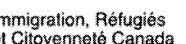
What is Lighthouse (a.k.a. Watchtower)?

Lighthouse is a prototype system that automatically and comprehensively extracts risk and fraud patterns from data, providing timely and actionable information to IRCC.

It DOES NOT recommend or make an administrative decision about a client.

Pages 62 to / à 65

are withheld pursuant to sections

sont retenues en vertu des articles

16(1)(b), 16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Value Proposition of Lighthouse

Flexible	Built in-house and is readily adaptable to other IRCC business lines
Comprehensive	System can scan for almost all forms of data-detectable risk patterns, and be configured for specific risk types (e.g., misrep, organized crime, etc.) or countries
Proactive	Able to identify new risk patterns, thus enabling Risk Assessment Units (RAUs) to proactively select cases for verifications, based on previous indicators
Effective	Enables RAUs and investigative teams to be more efficient and effective in identifying, validating and taking action on fraud and risk patterns
Improve Processing	Can contribute to improving processing speed of bona-fide applications
Cost savings	Cost avoidance from fewer adverse events (e.g., each asylum claim costs the federal government roughly $16,000)
Complementary	Dovetails with existing intelligence-based risk detection approaches
Inexpensive	Modest costs for development and maintenance. Immediately deployable using existing infrastructure

A3745417_7-000066

PILOT (GLOBAL SP)

Pages 68 to / à 69

are withheld pursuant to sections

sont retenues en vertu des articles

16(1)(b), 16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Immigration, Refugees   Immigration, Réfugiés
and Citizenship Canada   et Citoyenneté Canada

Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

s.16(1)(b)
s.16(1)(c)

Pilot Considerations: System complements human decision making

System provide neutral, factual information to increase evidence available to officers

- Lighthouse only provides information to support RAO decisions about when to collect additional evidence.
- No decision automation.
- All data used by the system originates from GCMS

Key Design Principle:
Lighthouse does not automate decisions, and does not affect processing of legitimate, non-adverse applications

The pilot is designed to avoid fettering

- Lighthouse information is only provided to risk assessment units for their consideration; adjudicating officers will not see Lighthouse pattern information and will not be informed which applications are involved in the pilot.

DEMO

Page 72

is withheld pursuant to sections

est retenue en vertu des articles

16(1)(b), 16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Lighthouse Live Pattern/Match Review Session

September 1, 2021 (CN/DN)

Sept 3, 2021 (IN)

Agenda

Housekeeping & Updates

- Questions from Intro Meeting?
- ADM Presentation
- Target Launch Date for soft launch start: Week of Sept 13, 2021
- User Manual Developed
  (https://gcdocs2.ci.gc.ca/otcs/cs.exe/link/414438888)
- Project Team Plans for interaction (IN, CN/DN, Project Steering)
- Planning: Charter Updates, Assessment Framework

Part 1: Review of the Lighthouse Weekly Report
(https://gcdocs2.ci.gc.ca/otcs/cs.exe/link/416335630)

- Column explanations
- Pattern Report Details
- Group inspection of a few matches

Part 2: Group Preparedness Discussion

Immigration, Refugees
and Citizenship Canada

Immigration, Réfugiés
et Citoyenneté Canada

Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

Key Questions

Comfort Level - Tool Usage

- How comfortable is the team with usage of the tool?

Comfort Level - Pilot Design

- How comfortable are users with the process as proposed and the start date of Week of Sept. 13, 2021?

Resource Availability

- Is it anticipated that resources will be available to support throughout the pilot?
- Do users need additional support to justify and brief upward on the project or their participation?

Preparedness

- Are there any additional considerations relating to planning, documentation, consultation, process definition, etc., which should be covered pre-launch? (e.g., assessment criteria)

Immigration, Refugees
and Citizenship Canada

Immigration, Réfugiés
et Citoyenneté Canada

Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

BIAS ASSESSMENT

Lighthouse

Prepared by:
Advanced Analytics Solutions Centre (A2SC)

Date: 2021-06-15

Immigration, Refugees   Immigration, Réfugiés
and Citizenship Canada   et Citoyenneté Canada
Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

s.16(1)(b)

s.16(2)(c)

1. Purpose

The purpose of this document is to make an initial assessment of the potential for bias under the Lighthouse Risk Identification System

2. Context

In the case of Lighthouse, which is designed to augment human decision making by identifying and summarizing possible historical patterns of concern, so that IRCC officers can make informed decisions about when additional scrutiny of an application may be required.

In the context of this project design, the primary focus of interest is on reducing the impact of "false positive" scenarios. In the context of the Lighthouse pilot, a false positive event occurs when a new applicant to IRCC matches against a historical pattern of concern identified by the lighthouse system. This event triggers a summary of this pattern to be shown to a Risk Assessment Officer, who assesses the pattern of concern summary, as well as the new application, to make a determination if additional information should be collected to ensure that supporting documentation submitted with an application is genuine and accurate.

This is important as the core reason for assessing bias for Lighthouse is to ensure that specific groups of individuals are not disproportionately impacted by the system.

3. Design Mitigation Considerations

A3745421_2-000077

Immigration, Refugees   Immigration, Réfugiés
and Citizenship Canada   et Citoyenneté Canada
Information disclosed under the Access to Information Act
s.16(1)(b) L'information divulguée en vertu de la loi sur l'accès à l'information
s.16(2)(c)

In developing the Lighthouse project, the Lighthouse Project Team has identified a pilot design that is intended to negate or greatly reduce any possible harm to any individual applicant that is not engaged in fraud or misrepresentation on their application. Put another way, the system is designed to reduce the human impact of a false positive to very close to zero. This design has important considerations as it relates to any potential system biases, as the core interest in bias assessment is to ensure that the system is not creating negative impacts that are disproportionately concentrated on a single demographic group. As designed, the system is intended to only impact true positive cases, i.e., applications that have been verified by a third-party as having submitted fraudulent documentation to support their application.

3.1. Mitigation 1: "Do No Harm" Design

Without proper mitigations, there are two clear ways that individuals who are not engaged in fraud on their applications could be negatively impacted by the system. These are the aforementioned false-positive cases.

a) **Processing Delays:** Without proper mitigations, the time it takes to verify with a third-party that a student is genuine could lead to delays in the processing of that person's applications. In the context of bias assessment, this could manifest itself in creating systematically longer processing times for women than men, for example.

b) **Refusal Likelihood:** Without mitigations, the Lighthouse system could create situations where individuals belonging to certain demographic groups may be systematically more likely to be refused, disproportionate to their actual underlying risk

Mitigating Processing Delays:

3.2. Mitigating Refusal Likelihood:

A more important risk to mitigate is the possibility that a legitimate applicant, who is not engaged in fraud or misrepresentation, is identified by the Lighthouse system and that merely by virtue of being identified by the system, they are viewed by officers as higher risk. This can result in a fettering of officer decisions and a negative impact on the client via a reduced likelihood of being approved.

This risk is mitigated in two ways. The first is to ensure that no information from lighthouse is ever used directly in front-line decision making. The second is by blinding the front-line officer to the fact that Lighthouse identified a possible concern on this application.

3.2.1. Lighthouse Information is never used directly in decision making and it does not automate decisions

As designed, Lighthouse provides information to

. This information takes the form of a neutral summary of a historical pattern of concern that matches the current application that has been received. This information performs only one purpose, which is to support a decision about whether additional validation of the applicants information should be performed.

information about past applications that identified the historical pattern of concern are never used as evidence in adjudicating a client's application. That is, there is no extrapolation of facts from past applications to the current application under consideration, only verified evidence about the application under consideration is used in the adjudication.

2.2. Mitigation of Decision Fettering

To ensure that Lighthouse pattern information is not inadvertently influencing application decisions, a separation is used between the Risk Assessment Officers (who assess Lighthouse information and decide if a verification should be performed on an application) and the Front-Line Officers who assess applications directly. The Front-Line Officers are not given access to Lighthouse information and are blinded to which applications have been identified by Lighthouse. This way, while Lighthouse may provide evidence about past fraud trends to help support the decision to verify facts of an application; it is ultimately the results of that third-party verification which are the sole piece of information made available to the front-line deciding officer.

Figure 1 visually describes the Lighthouse pilot design and these mitigation measures.

Figure 1: Pilot Design for Lighthouse

s.16(1)(b)

s.16(2)(c)

4. Quantitative Assessment of Bias

In the context of the SP pilot for Lighthouse, we believe that the previously noted mitigation measures greatly reduce any potential for the system to negatively impact any applicant that is not engaged in fraud. This is important context for bias assessment, as it is the systemic and uneven distribution of such negative impacts that are the primary measure of interest when assessing bias in a system such as Lighthouse.

Approach

To evaluate the historical bias assessment, Lighthouse was trained to identify patterns of concern on 799,000 student permit applications received by IRCC between January 1, 2019 to December 31, 2020 (training set). To support this bias assessment, the patterns identified in the training set were used to assess possible matches on an additional 276,000 applications received between January 1, 2021 and July 2, 2021 (test set).

Assessing Bias

Risk of fraud in IRCC applications is not evenly distributed amongst genders, age groups, or geographic regions. As such, it should not be expected that applications matching against historical risk patterns should be equally distributed among these same factors. Rather, it would be expected that the distribution of applications identified by the system as matching a historical pattern should roughly align with the underlying distribution of the known adverse applications in the historical data record. So, for example, in the training data assessed, men were 91% more likely than women to have an adverse verification on file, and were similarly 87% more likely than women to be identified as matching a historical pattern.

Gender Distributions

Gender Distributions

Males made up about 56% of student permit applications

s.16(1)(b)
s.16(2)(c)

Country of Residence Distributions

and similarly make up a large percentage of Lighthouse pattern match cases. The large number of countries that applicants reside in means that it is relatively unlikely to get an extremely close distribution between the matches produced by lighthouse and the underlying adverse distribution in these countries. However, a relatively close match was obtained, with the exception of some notable outliers.

. As a result, it appears that despite the high number of Lighthouse-matched applications relative to the baseline sample, the system does appear to have identified a growing fraud trend in this country that is being independently validated by the existing manual risk assessment work. As such, the system appears to be operating as intended. However, these trends will continue to be monitored closely throughout the pilot.
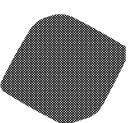
Age Distribution

s.16(1)(b)
s.16(2)(c)

A3745421_11-000086

Age Distribution

Lighthouses matches by age distribution very closely track to the baseline adverse distribution in the baseline population. Of note, individuals aged 26-35 may be slightly underrepresented relative to their share of adverse, but these appear to be within reasonable margins. It is worth noting that while

these individuals will be excluded from output during the pilot and will not be included in the system output reports provided to Risk Assessment Officers.

s.16(
Immigration, Refugees   Immigration, Réfugiés
and Citizenship Canada   et Citoyenneté Canada
Information disclosed under the Access to Information Act
s.16(2)(c)ation divulguée en vertu de la loi sur l'accès à l'information
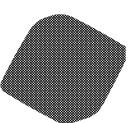
5. Summary

Overall, this bias assessment did not find significant evidence of bias in the outputs of Lighthouse patterns, and that Lighthouse matches relatively closely reflect underlying risk patterns present in the data.

It is important to note that any expected impact in terms of bias in the outputs of Lighthouse is expected to be greatly diminished or fully negated by the various mitigations discussed in this report. Most importantly, the pilot has been designed to ensure that any individual not engaged in fraud, even if identified by a match against a Lighthouse identified pattern of concern, should not be negatively impacted in any way.

Page 102

is withheld pursuant to sections

est retenue en vertu des articles

16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Page 103

is withheld pursuant to sections

est retenue en vertu des articles

16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Page 106

is withheld pursuant to sections

est retenue en vertu des articles

16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Page 107

is withheld pursuant to sections

est retenue en vertu des articles

16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Page 108

is withheld pursuant to sections

est retenue en vertu des articles

16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Page 109

is withheld pursuant to sections

est retenue en vertu des articles

16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Page 111

is withheld pursuant to sections

est retenue en vertu des articles

16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Page 114

is withheld pursuant to sections

est retenue en vertu des articles

16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Page 115

is withheld pursuant to sections

est retenue en vertu des articles

16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Page 116

is withheld pursuant to sections

est retenue en vertu des articles

16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Page 117

is withheld pursuant to sections

est retenue en vertu des articles

16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Pages 119 to / à 132

are withheld pursuant to sections

sont retenues en vertu des articles

s.16(1)(b), s.16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Page 119

is withheld pursuant to sections

est retenue en vertu des articles

16(1)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Page 120

is withheld pursuant to sections

est retenue en vertu des articles

16(1)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Page 122

is withheld pursuant to sections

est retenue en vertu des articles

16(1)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Page 133

is withheld pursuant to sections

est retenue en vertu des articles

16(1)(b), 16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Lighthouse (aka Watchtower) Project Updates

Global Risk & Fraud Pattern Detection

Advanced Analytics Solutions Centre (A²SC-OPPB)

July 2021

Canada

A3745429_1-000134

Purpose

1. Provide an overview of the A2SC-developed Lighthouse (previously known as Watchtower) Risk Identification System.

2. Outline plans for an operational pilot project, testing the use of the tool to improve program integrity and fraud detection efficiency in the global Student Permit (SP) caseload.

Immigration, Refugees   Immigration, Réfugiés
and Citizenship Canada   et Citoyenneté Canada
Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

What is Lighthouse (a.k.a. Watchtower)?

Lighthouse is a prototype system that automatically and comprehensively extracts risk and fraud patterns from data, providing timely and actionable information to IRCC.

It DOES NOT recommend or make an administrative decision about a client.

Pages 137 to / à 139

are withheld pursuant to sections

sont retenues en vertu des articles

s.16(1)(b), s.16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Page 140

is withheld pursuant to sections

est retenue en vertu des articles

16(1)(b), 16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Value Proposition of Lighthouse

Flexible	Built in-house and is readily adaptable to other IRCC business lines
Comprehensive	System can scan for almost all forms of data-detectable risk patterns, and be configured for specific risk types (e.g., misrep, organized crime, etc.) or countries
Proactive	Able to identify new risk patterns, thus enabling Risk Assessment Units (RAUs) to proactively select cases for verifications, based on previous indicators
Effective	Enables RAUs and investigative teams to be more efficient and effective in identifying, validating and taking action on fraud and risk patterns
Improve Processing	Can contribute to improving processing speed of bona-fide applications
Cost savings	Cost avoidance from fewer adverse events (e.g., each asylum claim costs the federal government roughly $16,000)
Complementary	Dovetails with existing intelligence-based risk detection approaches
Inexpensive	Modest costs for development and maintenance. Immediately deployable using existing infrastructure

A3745429_8-000141

DEMO

PILOTS

Pages 144 to / à 146

are withheld pursuant to sections

sont retenues en vertu des articles

s.16(1)(b), s.16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

KEY CONSIDERATIONS

Canada

Pilot Considerations: System complements human decision making

System provide neutral, factual information to increase evidence available to officers

- Lighthouse only provides information to support RAO decisions about when to collect additional evidence.

- No decision automation.

- All data used by the system originates from GCMS

Key Design Principle:

Lighthouse does not automate decisions, and does not affect processing of legitimate, non-adverse applications

The pilot is designed to avoid fettering

- Lighthouse information is only provided to risk assessment units for their consideration; adjudicating officers will not see Lighthouse pattern information and will not be informed which applications are involved in the pilot.

Immigration, Refugees
and Citizenship Canada

Immigration, Réfugiés
et Citoyenneté Canada

Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

THANK YOU!

QUESTIONS?

Page 152

is withheld pursuant to sections

est retenue en vertu des articles

16(1)(b), 16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Immigration, Refugees Immigration, Réfugiés
and Citizenship Canada et Citoyenneté Canada
Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

Annex: Participating Teams

Engaged Stakeholders

International Network (IN)

Domestic Network (DN)

Centralized Network (CN)

Integrity Risk Management (IRM)

Immigration Program Guidance (IPG)

Legal Services (Department of Justice/LSU)

Privacy (ATIP)

Strategic Planning and Performance (SPP)

Annex: Mitigation of Bias/Discrimination

- A2SC goes to great lengths to ensure that Lighthouse is developed responsibly and does not introduce bias.

- Steps include:

  1. External review of Lighthouse by Statistics Canada

  2. Following best practices in data science to avoid bias and active monitoring of risk indicators

  3. Many layers of human review of the risk patterns to eliminate incremental bias

  4. Overall design centred on the interests of the client to avoid causing harm

  5. Active engagement with external stakeholders, including governance exercise in Winter 2020

  6. Follow the comprehensive ethics framework to govern AA work

Immigration, Refugees   Immigration, Réfugiés
and Citizenship Canada   et Citoyenneté Canada

Canada

A3745429_21-000154

Immigration, Refugees Immigration, Réfugiés
and Citizenship Canada et Citoyenneté Canada
Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

Background

In Canada, privacy is considered a human right. As the majority of the data we handle at IRCC is personal information, privacy requirements must be top-of-mind when planning, developing and monitoring any initiative involving data-driven technology.

This document is intended to outline the privacy protections in place for this particular model or tool. The requirement statements in this document are based off the Baseline Privacy Requirements for Disruptive Technology that lays out the minimum privacy requirements that must be met for all initiatives involving disruptive technology.

This document **does not replace** the need for a Privacy Impact Assessment (PIA) as it is intended only to analyze privacy compliance at a model level and document steps taken to increase privacy protections. This document may be used to assist in completing a larger initiative or program-level privacy assessment as required. Program areas are responsible for filling out a Privacy Needs Assessment (PNA) and sending it to the ATIP Division. Information about the PNA and the template can be found on Connexion.

Details

Name of Initiative:	
Branch/Division who is responsible for the Model:	
Type of Model (triage, predictive, risk pattern identification, etc):	
Date model is expected to be launched:	
Version 1.0 Model Privacy Assessment is completed:	
Update MPA whenever the Model or Tool is updated	

Immigration, Refugees
and Citizenship Canada

Immigration, Réfugiés
et Citoyenneté Canada

Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

s.16(1)(b)

s.16(2)(c)

Model Privacy Assessment

Lighthouse – Study Permit Pilot #2

Version 1.0 Final – May 2021

Model or Tool Update Date:	
Version 2.0 Model Privacy Assessment completed:	

Summary of Initiative

What is the problem this model is trying to solve? Why is this the best solution to that problem? Why is the use of personal information necessary? What does the model do? What is the population the model is being applied to (ex: study permit applicants from a specific country)? In what way does the model support officers in making decisions? Does it suggest decisions for officers? Please include any and all useful information.

Summary of Initiative
Lighthouse is a prototype risk detection tool developed by IRCC's Advanced Analytics Solution Centre (A2SC). The tool aims to enhance program integrity and Canadian public safety by automatically identifying and summarizing historical risk patterns for IRCC officials. The tool aims to provide neutral, fact-based risk information to IRCC officials, augmenting their capacity to quickly identify and understand organized fraud trends and other risk patterns. It can be used to support frontline decision makers or to understand historical risk patterns. Lighthouse presents opportunities for the department to modernize IRCC's risk assessment activities by placing timely and relevant risk information at the fingertips of IRCC officials in a manner that was previously impossible or prohibitively expensive to do.

Immigration, Refugees and Citizenship Canada

Immigration, Réfugiés et Citoyenneté Canada

Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

s.16(1)(b)

s.16(2)(c)

Model Privacy Assessment

Lighthouse – Study Permit Pilot #2

Version 1.0 Final – May 2021

Immigration, Refugees
and Citizenship Canada
Immigration, Réfugiés
et Citoyenneté Canada

Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information
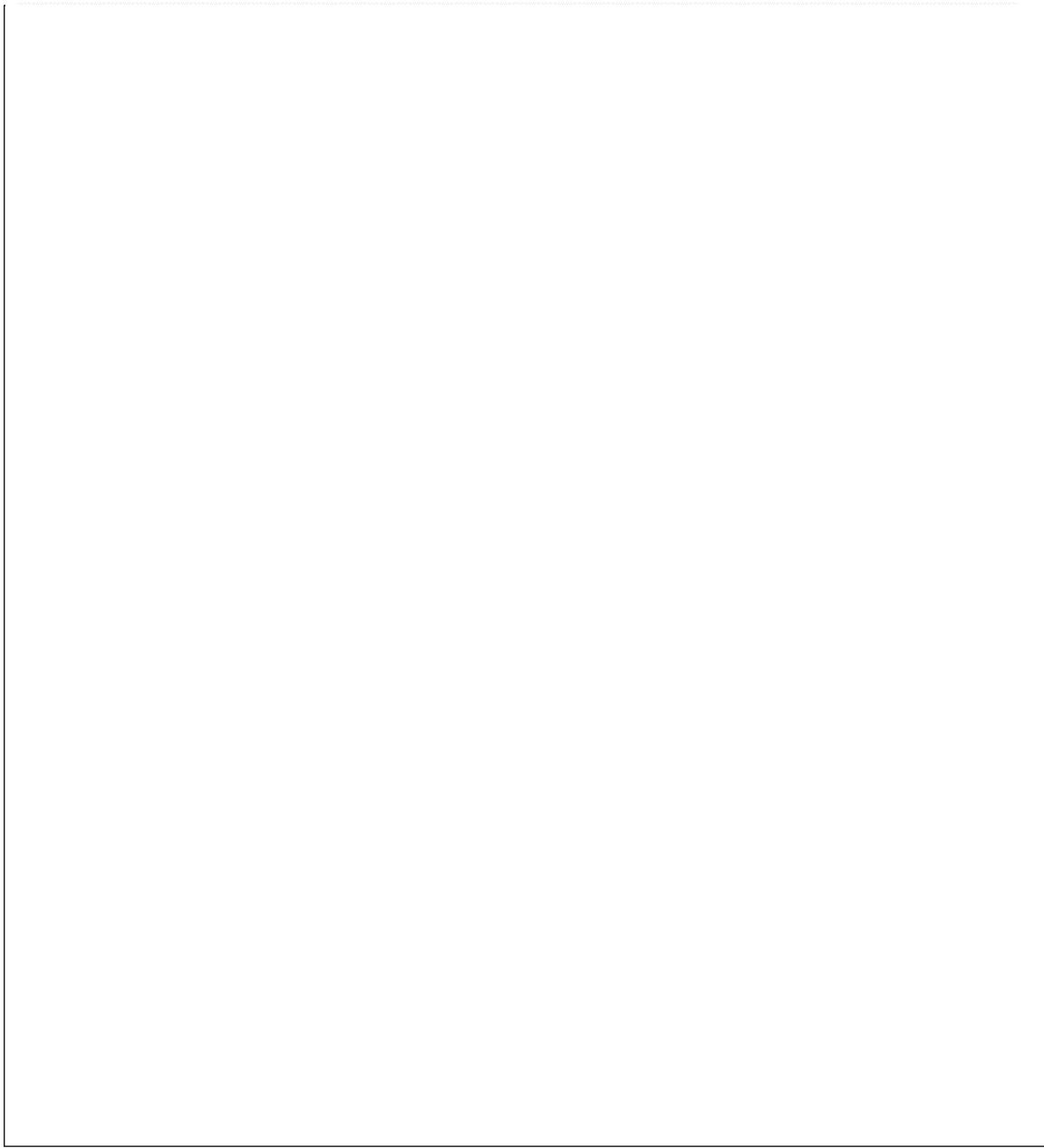
s.16(1)(b)

s.16(2)(c)

Model Privacy Assessment

Lighthouse – Study Permit Pilot #2

Version 1.0 Final – May 2021

High-Level Summary of How the Model Works (as appropriate, include: how the rules are created, how an application runs through a model/how personal information is used in production, an overview of the output/what officers see, etc.)

Immigration, Refugees
and Citizenship Canada

Immigration, Réfugiés
et Citoyenneté Canada

Model Privacy Assessment

Lighthouse – Study Permit Pilot #2

Version 1.0 Final – May 2021
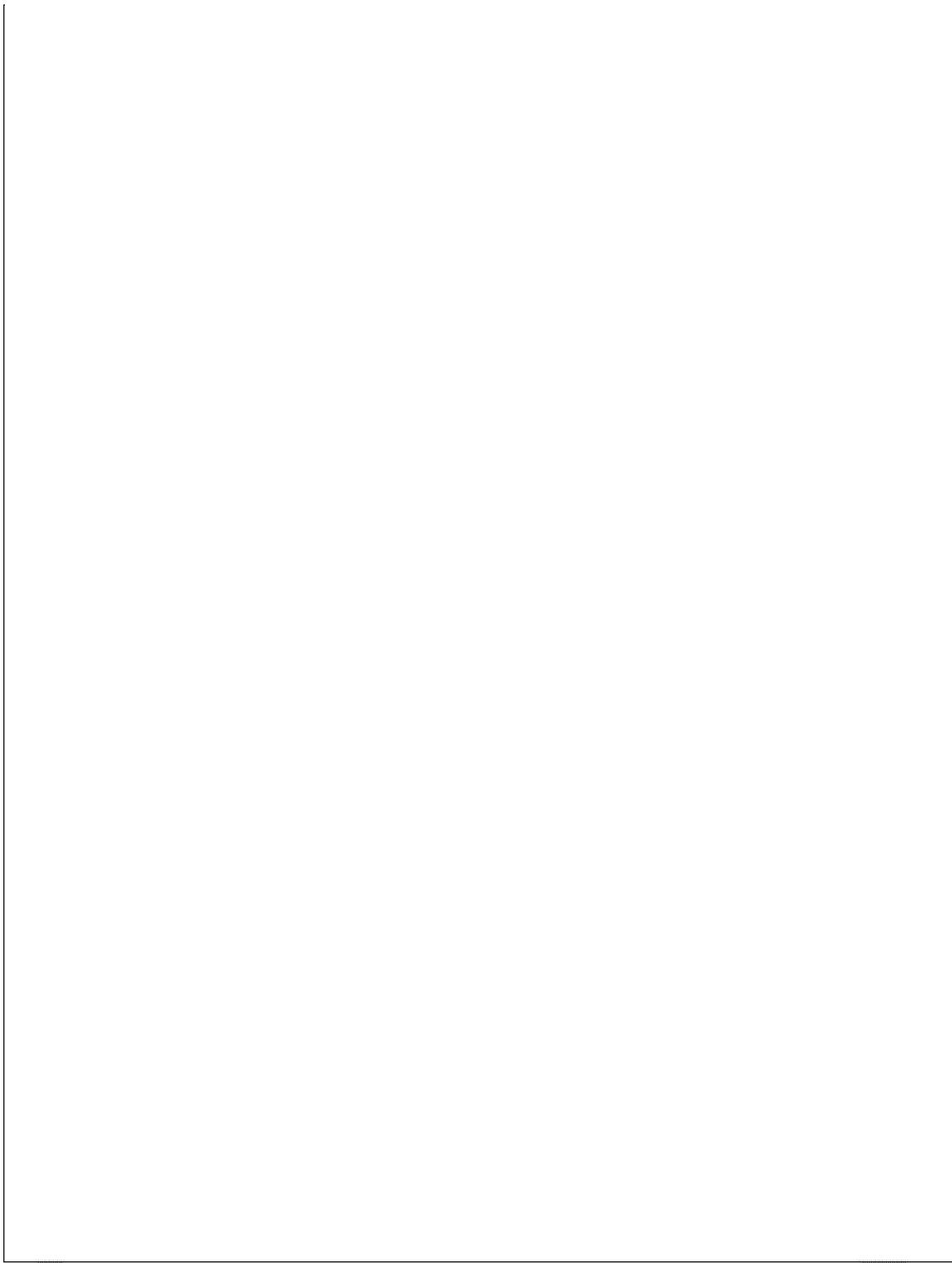
Model Privacy Assessment

Lighthouse – Study Permit Pilot #2

Version 1.0 Final – May 2021

Requirements

Legal Authority

A program must have the parliamentary authority to collect and use personal information for the specified purposes of the program. This legal authority will be identified in the Privacy Needs Assessment and other required privacy assessments for this initiative.

A program must also be legally allowed to use disruptive technology and/or automation to support the program. Identify which of the legal authorities below grant your program area the **authority to administer your program(s) using electronic means** (disruptive technology):

☒ Part 4.1 of the Immigration Refugees Protection Act

☐ Section 2.2 of the Passport Order

Accountability

A part of ethical and responsible development and deployment of advanced analytics, artificial intelligence and automation initiatives is ensuring that **humans are ultimately responsible for the model's behaviour.** Describe below the processes to guarantee that

model rules are reviewed by humans and to make sure that internal governance and accountability (sign-off) processes are in place.

s.16(1)(b)

s.16(2)(c)

Model Privacy Assessment

Lighthouse – Study Permit Pilot #2

Version 1.0 Final – May 2021
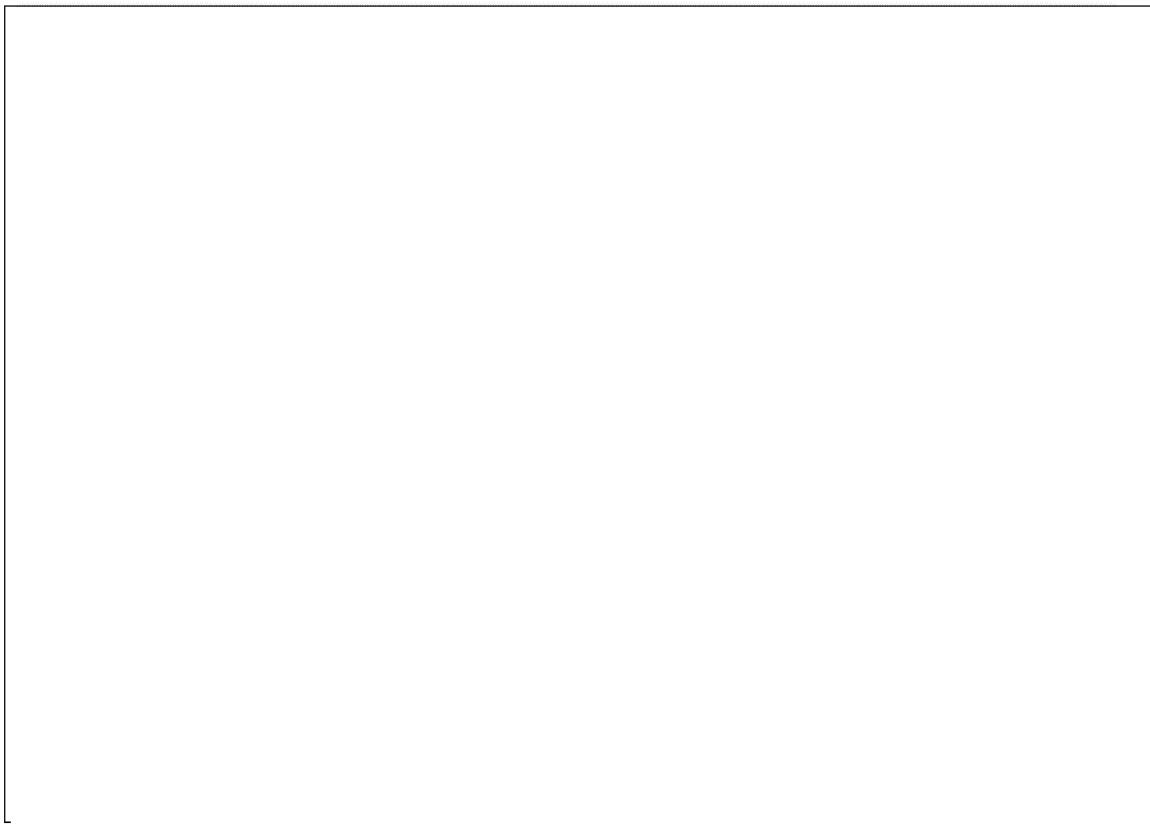
Source of Data

Personal information must only be collected if it relates directly to an operating program or activity of IRCC and each personal information data element must be necessary to the administration of the program. When possible, personal information should be collected directly from the individual.

For the purposes of disruptive technology initiatives, **only information found in departmental systems of record (ex. GCMS) should be used** unless another data source has been approved by IT Security, and the activities of training models and algorithms should be done outside of those systems of record. Data collected from outside sources should not be used unless demonstrably necessary, and proper information sharing

Privacy, Policy and Governance Unit, ATIP Division | June 2021 | Version 1.0 – Final

8

A3745437_8-000164

Immigration, Refugees
and Citizenship Canada
Immigration, Réfugiés
et Citoyenneté Canada
Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

Model Privacy Assessment

Lighthouse – Study Permit Pilot #2

s.16(1)(b)

s.16(2)(c)

Version 1.0 Final – May 2021

agreements, memoranda of understanding, service level agreements etc. should be in place and followed.

Source of Data – Where the data comes from and reasonableness of using that data	
Source of the data (ex: GCMS)	
If outside data is used, through what means is it collected (ex: MOUs, ISAs, etc.)	
Demonstrate how Necessity, Proportionality, Effectiveness, and Minimal Intrusiveness, were considered and applied in considering what data to use in the model (Oakes Test).	

s.16(1)(b)
s.16(2)(c)

Immigration, Refugees
and Citizenship Canada

Immigration, Réfugiés
et Citoyenneté Canada

L'information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

Model Privacy Assessment

Lighthouse – Study Permit Pilot #2

Version 1.0 Final – May 2021
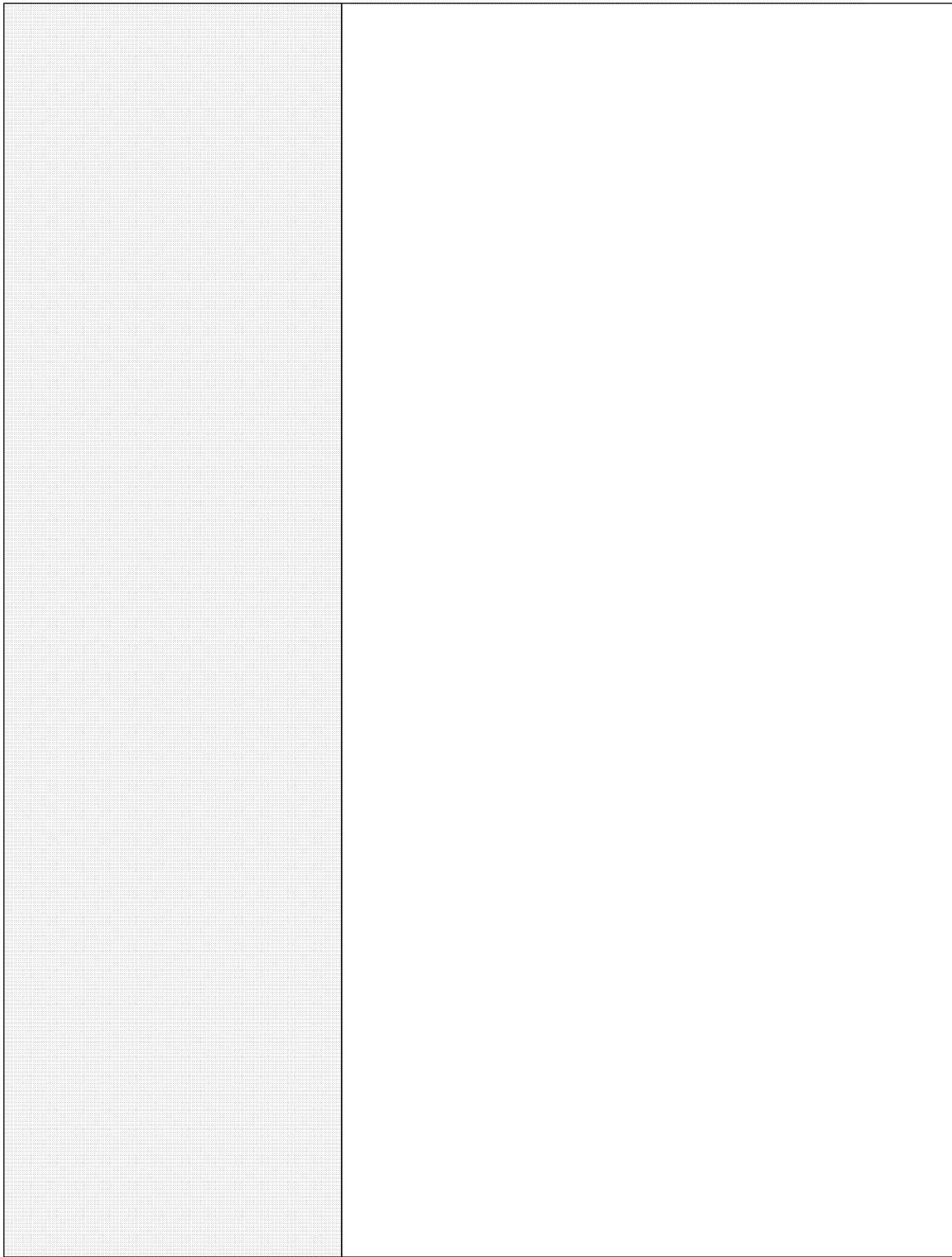
s.16(1)(b)
s.16(2)(c)

Model Privacy Assessment

Lighthouse – Study Permit Pilot #2

Version 1.0 Final – May 2021

Notice / Informed of Purpose / Transparency / Explainability

IRCC must notify individuals (clients and the general public) of the purpose for which their information is being collected, commonly referred to as a 'privacy notice.' This notice must be given at or before the time of collection. IRCC must notify past applicants that their information was used to train or build models. Individuals have a right to know exactly how their personal information was processed through a disruptive technology system. Ensuring that plain language explanations are available on demand would allow individuals to see how technology was used to support decision-making.

Notice & Transparency – How individuals (clients and the general public) will be notified about the use of this model and how the use of disruptive technology will be explained to applicants.	
Notice at time of collection (link to the privacy notice if applicable)	The privacy notice on the Study Permit forms a well as the corresponding Personal Information Bank (PIB) have been updated to account for the use of analytics.
Transparency to historical applicants and public	The Digital Transparency webpage that is now published accounts for the use of risk screening tools such as Lighthouse by explaining that advanced data analytics systems will be used by IRCC to recognize patterns to help accelerate our work and better inform decision makers.

Immigration, Refugees Immigration, Réfugiés
and Citizenship Canada et Citoyenneté Canada
Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

Model Privacy Assessment

Lighthouse — Study Permit Pilot #2

s.16(1)(b)

s.16(2)(c)

Version 1.0 Final — May 2021

Explainability of the model (link to the plain language explanation)	The pattern reports that are used in Lighthouse are intended to provide sufficient evidence of any individual pattern. All patterns are "self-contained" in that they are intended to stand on their own merit regardless of the rest of the system. Encrypted data and model information is currently being retained to allow A2SC to recreate a model on-demand and provide the underlying data to explain how Lighthouse patterns were produced and why applications matched against these patterns.

Accuracy

IRCC must take all reasonable steps to ensure that personal information used for an administrative purpose is as **accurate, up-to-date and complete as possible**. This also includes ensuring there are mechanisms to correct inaccurate information.

For initiatives involving disruptive technology, this involves ensuring data is collected from a reliable source, the quality of the data, developing technological mechanisms to make certain that the technology is working (such as feedback loops and blind tests), quality assurance on the outputs, and so on. Additionally, to guarantee the accuracy of the data, program areas must take the necessary steps to minimize unintended bias in the data. Finally, accuracy also involves model maintenance and ensuring the model is trained and re-trained on the most updated, accurate and reliable data.

Accuracy – Ways the model is ensuring accuracy of the data and outputs, and the process to correct inaccuracies. Describe any Quality Assurance (QA) processes that are in place.

A3745437_12-000168

s.16(1)(b)

s.16(2)(c)

Model Privacy Assessment

Lighthouse – Study Permit Pilot #2

Version 1.0 Final – May 2021

Use

Personal information must only be used for the purpose it was initially collected, a use consistent with that purpose or for a purpose for which it is may be disclosed under section 8(2) (see Disclosure, below).

Applying disruptive technology to a dataset involving personal information is a use; this includes all uses whether administrative or not. Personal information must be treated appropriately regardless of the level of automation or support the technology is providing. The use of disruptive technology should be a consistent use of the personal information. To determine what constitutes a consistent use of personal information, the original purpose and the proposed purpose must be so closely related that the individual would expect that the information would be used for the consistent purpose, even if the use is not spelled out.

Immigration, Refugees
and Citizenship Canada
Immigration, Réfugiés
et Citoyenneté Canada
Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

Model Privacy Assessment

Lighthouse – Study Permit Pilot #2

s.16(1)(b)

s.16(2)(c)

Version 1.0 Final – May 2021

Use – Mechanisms that are in place to reduce the inappropriate use of the data	
Confirmed that applying this model is a consistent use of the personal information (provide the text from the legal opinion if applicable at time of completing this assessment)	
Data minimization (only use data elements that are absolutely necessary)	
Reducing data granularity (removing precision of some data elements, ex: using only the first three digits of a postal code)	
De-identification (masking/hashing/synthesizing	

s.16(1)(b)

s.16(2)(c)

Model Privacy Assessment

Lighthouse – Study Permit Pilot #2

Version 1.0 Final – May 2021

data so that it's no longer personally identifiable)	
Need to Know (ensuring access is only granted to those who need to know it)	
Other (Ex: Use of privacy enhancing technologies, anonymizing data for all demonstrations, etc)	

Disclosure

Personal information under IRCC's control must not be disclosed to anyone or any organization for any reason, except for those reasons listed in sub-section 8(2) of the *Privacy Act*.

A3745437_15-000171

Model Privacy Assessment

Lighthouse – Study Permit Pilot #2

Version 1.0 Final – May 2021

For initiatives involving disruptive technology, this includes information found in departmental systems of record (ex. GCMS) that other organizations such as CBSA or CSIS can view. Regular information sharing may continue to occur between IRCC and partner organizations, however Memoranda of Understanding (MOUs), Information Sharing Agreements (ISAs) and other formal agreements must be updated and modified through the appropriate channels if there is the desire to disclose outputs on a regular basis.

Disclosure – Mechanisms that are in place to reduce the risk of inappropriate disclosure of the data, outputs and other model-related personal information. List GC partners and MOUs ISAs linked to this project as applicable.

Model Privacy Assessment

Lighthouse – Study Permit Pilot #2

Version 1.0 Final – May 2021

Safeguards

Personal information must be safeguarded appropriately regardless of the kind of technology applied to it. **Appropriate administrative, technical and physical safeguards should be applied to personal information at all stages of a disruptive technology initiative,** and consideration should be given to reducing the likelihood of privacy and security breaches throughout development.

Safeguards – Safeguards that are in place in and around the model to protect the data

Immigration, Refugees
and Citizenship Canada
Immigration, Réfugiés
et Citoyenneté Canada

Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

Model Privacy Assessment

Lighthouse – Study Permit Pilot #2

s.16(1)(b)

s.16(2)(c)

Version 1.0 Final – May 2021

Retention and Disposal

Personal information used for an administrative purpose (as a part of a decision-making process that affects the individual) must be retained for at least two years, and in accordance with the appropriate Retention and Disposition Schedule. All data (with the exception of training data in the Exploration Zone) must be kept such that in the event of a complaint or legal action, the decision can be replicated. The data in the Exploration Zone that is an exact duplicate of production data and that is used to generate and retrain model rules can be considered transitory.

Retention and Disposition schedules	
Training Data in EZ	
Client Input Data (during production)	
Model Outputs	

A3745437_18-000174

Immigration, Refugees
and Citizenship Canada

Immigration, Réfugiés
et Citoyenneté Canada

Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

Model Privacy Assessment

Lighthouse – Study Permit Pilot #2

Version 1.0 Final – May 2021

Model (the code)	
Reports (outputs for officers, legal tables, others as appropriate)	

Monitoring Plan

Monitoring for privacy compliance to the above-noted requirements should be built in from the model development phase and a monitoring schedule post-deployment should be followed.

In addition to being certain that the disruptive technology is working properly, here is a list of non-exhaustive monitoring activities to plan for:

- **Collection**: Make sure no data from sources other than departmental systems of record (ex. GCMS) and other IRCC data repositories are included in the disruptive technology, and if there is outside data, put in place the appropriate ISA or MOU and keep these up to date.
- **Notice**: Review privacy notices and transparency and explainability practices for accuracy and for current information. Update when required.
- **Retention and Disposal**: Review the retention and disposal practices and ensure that no information is retained beyond IRCC's prescribed retention period.
- **Accuracy**: Build in regular data quality practices to ensure data is accurate, up to date and as complete as possible, and modify the information when required.

A3745437_19-000175

Immigration, Refugees   Immigration, Réfugiés
and Citizenship Canada   et Citoyenneté Canada

Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

s.16(1)(b)

s.16(2)(c)

Model Privacy Assessment

Lighthouse – Study Permit Pilot #2

Version 1.0 Final – May 2021

- **Use**: Review data handling practices, ensure mitigation measures against inappropriate use are functioning properly, employ new measures as required, and update practices periodically.

- **Disclosure**: Review disclosure practices so that disclosures are occurring as a part of up to date MOUs and/or ISAs, and ensure other government organizations can only see information they are permitted to see in GCMS under those MOUs/ISAs. Make modifications when required.

- **Safeguards**: Complete the mandatory IT Security Assessment and Authorization process and conduct security checks to confirm that the training data, the technology itself and the outputs are secure.

> **Monitoring** – Monitoring for privacy compliance once the model is in production. Please describe the steps you will follow to develop and establish the required monitoring plan.

A3745437_20-000176

Immigration, Refugees   Immigration, Réfugiés
and Citizenship Canada   et Citoyenneté Canada
Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

s.16(1)(b)

s.16(2)(c)

Model Privacy Assessment

Lighthouse – Study Permit Pilot #2

Version 1.0 Final – May 2021

Monitoring Notes:

The quality assurance and monitoring plans will monitor the ongoing efficacy of the model and of the data quality. The quality assurance and monitoring activities will contribute to monitoring the Accuracy and Use privacy requirements. At the time of completing this document, a detailed plan to monitor all of the privacy requirements was not in place. However, the measures that are in place should mitigate many potential privacy risks in the future (such as encrypting data, limiting access to only those with a 'need to know' etc.) This model will be in a pilot mode from June 2021 to October 2021, and many assessments will take place during that time. Building in additional privacy controls may occur during the pilot and they will be recorded in future versions of this document.

As of June 2, 2021, a formal plan to monitor the privacy requirements for the Lighthouse model has not been completed.

Gap Analysis and Proposed Recommendations

Requirement	Gap	Proposed Recommendation	Status
Retention and Disposal	No clear retention and disposal schedules have been determined.	Meet with IM to determine a retention and disposal schedule for all Lighthouse data.	Not begun – to engage with IM in the coming weeks

Immigration, Refugees   Immigration, Réfugiés
and Citizenship Canada   et Citoyenneté Canada
Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

Model Privacy Assessment

Lighthouse — Study Permit Pilot #2

Version 1.0 Final — May 2021

Monitoring	A clear plan to monitor the effectiveness of privacy controls and adherence to privacy requirements.	Currently quality assurance mechanisms are in place to monitor the accuracy and effectiveness of the model. However, Privacy recommends that a more detailed monitoring plan be developed to monitor adherence to privacy requirements or include it in existing documentation.	Not begun

Documents Reviewed to Gather Information

The documents below are linked to their source in GCDOCS. As future readers of this MPA may not have access to those documents, below is a point-in-time capture of the documents as of May 20, 2021. Because they are point-in-time, note that they may be drafts, so please use the hyperlink when possible.

1. Lighthouse Privacy Needs Assessment -

   http://gcdocs2/otcs/cs.exe?func=ll&objaction=overview&objid=392470772

   A2SC - PNA -
   Lighthouse for SP.d

2. Lighthouse Project Charter -

   http://gcdocs2/otcs/cs.exe?func=ll&objaction=overview&objid=389516701

A3745437_22-000178

Model Privacy Assessment

Lighthouse – Study Permit Pilot #2

Version 1.0 Final – May 2021

A2SC - Project
Charter - Lighthouse

3. Lighthouse Study Permit Pilot Legal Opinion -

    http://gcdocs2/otcs/cs.exe?func=ll&objaction=overview&objid=392337429

Lighthouse Study
Permit Pilot Legal Op

Signature

Invalid signature

X _Tracy Perry_
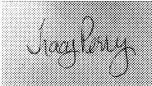
Tracy Perry
ATIP Director
Signed by: Perry, Tracy

A3745437_23-000179

Major Recommendations

Pages 181 to / à 182

are withheld pursuant to sections

sont retenues en vertu des articles

s.16(1)(b), s.16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Immigration, Refugees
and Citizenship Canada
Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

Immigration, Réfugiés
et Citoyenneté Canada

s.16(1)(b)
s.16(2)(c)

Minor Recommendations

Immigration, Refugees
and Citizenship Canada
Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

Immigration, Réfugiés
et Citoyenneté Canada

s.16(1)(b)
s.16(2)(c)

A3745440_4-000183

Response

Agreed. We will develop a few descriptive use-case stories/scenarios to make the usage transparent and clear, and include a process-flow diagram in the documentation to clarify the intended pilot use-case for the tool.   In addition, we will add additional documentation defining the types of adverse information used by the system. Under the planned pilot,

officer; the tool summarizes information from IRCC's database to help inform that decision.

The report was written this way to keep it relevant to a lay audience, but we can make these changes.

We will make adjustments to this wording to clarify where the system is predictive in nature. To clarify, the tool does not make recommendations and is not used directly in influencing administrative decision making on applications.   It does not make recommendations or provide predictive scores, but rather summarizes factual information from ircc's data holdings on applications where a possible concern is identified.   There is a predictive aspect in the sense that information is not shown on all applications, but rather only those that have some possible concern as identified in the data.

As a demonstrative example: A simple univariate pattern example might be a case where the system presents the following information to a user: '

While an algorithm was used to identify that this information exists in IRCC's data holdings, the factual information presented is designed to stand entirely on its own merits as evidence to inform a decision about whether additional information should be collected from

. No trust or reliance is ever placed in the algorithm itself to drive a decision or present a recommendation, and decision making is solely based on factual information collected about the specific applicant, and is never influenced by extrapolation of facts from a past trend (i.e., prediction). This is the key point we are trying to highlight in differentiating the approach from a traditional binary classifier or predictive system.

For added context, the current existing business at IRCC for verifying application information is roughly the same

Immigration, Refugees and Citizenship Canada

Immigration, Réfugiés et Citoyenneté Canada

Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

This will be added to the report. Our general approach to bias/fairness is to ensure ongoing monitoring in the course of some relatively small low-risk piloting of the system (currently being considered for approval). Bias monitoring (primarily looking at distribution of false positive rates across demographic variables) is also built into the ongoing monitoring assessment.

On the question of stereotypes, a major mitigation is the design of this pilot work, which will only use evidence from neutral non-subjective third-party sources of information. To illustrate, the general use-case put forward is as follows:

An applicant for a student permit raises a possible fraud concern by the system. A summary of the historical pattern is generated for a risk assessment officer, which shows that an application for a student permit shares similarities to a dozen other past applications that have used forged acceptance letters from "fakeSchoolName University" to try to enter Canada. The officer notices that this applicant also plans to study at fakeSchoolName and decides to verify with the school that this person is in fact enrolled there. They perform a verification by contacting the school to determine that the individual is enrolled. This response from the school will be assessed when deciding whether to approve or refuse the application. Of note, the officer that performs the verification and the officer that makes the decision on the application are different individuals. To avoid any fettering/biasing concerns, the officer making the decision does not see any output from the system and is not aware that it was used on this application.   They have no knowledge of the 12 similar past applicants that committed fraud. As such, the decision is only influenced by factual "yes/no" evidence obtained from the school. As required, the decision is based solely on evidence specific to this exact applicant, and never on the basis of the 12 similar applicants who committed fraud in the past.

This is the sole usage of the system considered for testing at present. We believe that this design effectively mitigates any concerns around bias or the perpetuation of stereotypes. Even if bias or stereotypes were present in the verifying officer, and this influences the decision to perform a verification, there is no room for this to influence the final decision on an application.

This will be added to the report. The high-level plan is to regularly shift the time-window in which patterns are assessed, as well as to qualitatively assess the utility of the tool for risk assessment officers. This will ensure that the system is always displaying relevant and timely data and that stale information is not being presented. Future mitigations will be required to ensure that the system, once in production, does not self-reinforce on its past results. We have had some preliminary discussions about the possibility of using random sampling methods

This will be added to the report.

Agreed. We are working with comms team on communications strategies.

Agreed. Please see the point six above about the impact on clients of false positives (increased approval likelihood). We believe this would make some of the policing examples poor direct comparables, as these typically have significant negative impacts in the event of false positives. We will examine the research and draw

Lighthouse (aka Watchtower) Project Updates
Global Risk & Fraud Pattern Detection

Advanced Analytics Solutions Centre (A^{2}SC-OPPB)

September 2021

Purpose

1. Provide an overview of the A2SC-developed Lighthouse (previously known as Watchtower) Risk Identification System.

2. Outline plans for an operational pilot project, testing the use of the tool to improve program integrity and fraud detection efficiency in the global Student Permit (SP) caseload.

Immigration, Refugees   Immigration, Réfugiés
and Citizenship Canada   et Citoyenneté Canada
Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

What is Lighthouse (a.k.a. Watchtower)?

Lighthouse is a prototype system that automatically and comprehensively extracts risk and fraud patterns from data, providing timely and actionable information to IRCC.

It DOES NOT recommend or make an administrative decision about a client.

A3745441_3-000190

Pages 191 to / à 192

are withheld pursuant to sections

sont retenues en vertu des articles

s.16(1)(b), s.16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Immigration, Refugees
and Citizenship Canada

Immigration, Réfugiés
et Citoyenneté Canada

Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

Value proposition

Flexible	Can be adapted to other IRCC business lines
Comprehensive	Can scan for many forms of data-detectable risk patterns, and can be configured for specific countries or risk types (e.g., misrep, organized crime, etc.)
Effective	Enables RAUs and investigative teams to be more efficient and effective in identifying, validating and taking action on fraud and risk patterns
Improve Processing	Improves timeliness of verifications, thereby preventing delays in processing for a small number of files
Cost savings	Cost avoidance from fewer adverse events (e.g., each asylum claim costs the federal government roughly $16,000)
Complementary	Dovetails with existing intelligence-based risk detection approaches
Inexpensive	Modest costs for development and maintenance. Immediately deployable using existing infrastructure

A3745441_6-000193

Pages 194 to / à 195

are withheld pursuant to sections

sont retenues en vertu des articles

s.16(1)(b), s.16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Immigration, Refugees   Immigration, Réfugiés
and Citizenship Canada   et Citoyenneté Canada
Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

s.16(1)(b)
s.16(2)(c)

System complements human decision making

System provide neutral, factual information to increase evidence available to officers

- Lighthouse only provides information to support RAO decisions about when to collect additional evidence.

- No decision automation.

- All data used by the system originates from GCMS

Key Design Principle:

Lighthouse does not automate decisions, and does not affect processing of bona fide applications

-

The pilot is designed to avoid fettering

- Lighthouse information is only provided to risk assessment units for their consideration.

- Adjudicating officers will not see Lighthouse risk patterns.

A3745441_9-000196

Pages 197 to / à 198

are withheld pursuant to sections

sont retenues en vertu des articles

s.16(1)(b), s.16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

ANNEX

Annex: Participating Teams

Engaged Stakeholders

Integrity Risk Management (IRM) – **Business Owner**

International Network (IN)

Domestic Network (DN)

Centralized Network (CN)

Immigration Program Guidance (IPG)

Legal Services (Department of Justice/LSU)

Privacy (ATIP)

Strategic Planning and Performance (SPP)

A3745441_13-000200

Annex: Mitigation of Bias/Discrimination

- A2SC goes to great lengths to ensure that Lighthouse is developed responsibly and does not introduce bias.

- Steps include:

  1. External review of Lighthouse by Statistics Canada

  2. Following best practices in data science to avoid bias and active monitoring of risk indicators

  3. Many layers of human review of the risk patterns to eliminate incremental bias

  4. Overall design centred on the interests of the client to avoid causing harm

  5. Active engagement with external stakeholders, including governance exercise in Winter 2020

  6. Follow the comprehensive ethics framework to govern AA work

A3745441_14-000201

Pages 202 to / à 203

are withheld pursuant to section

sont retenues en vertu de l'article

s.16(1)(b), s.16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Pages 204 to / à 211

**are withheld pursuant to section**

sont retenues en vertu de l'article

s.16(1)(b), s.16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Page 212

is not relevant

est non pertinente

Pages 213 to / à 226

are withheld pursuant to sections

sont retenues en vertu des articles

s.16(1)(b), s.16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Page 224

is withheld pursuant to sections

est retenue en vertu des articles

21(1)(d), 21(1)(b)

of the Access to Information Act

de la Loi sur l'acces a l'information

Pages 227 to / à 241

are withheld pursuant to sections

sont retenues en vertu des articles

s.16(1)(b), s.16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

APPENDIX C

16

Search:

COUNT

Show 50 ⌄ entries

Search:

Pages 259 to / à 264

are withheld pursuant to sections

sont retenues en vertu des articles

s.16(1)(b), s.16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

26

TIMELINE   ADVERSE BREAKDOWN   NOTE DETAILS   VERIFICATIONS

Show 50 ⌄ entries   Search: [   ]

VERIF_RESULT	VERIF_CREATED	VERIF_DOC_TYPE	VERIF_DOC_SUBTYPE	VERIF_DOC_TYPE_OTHER	VERIF_DESC_TXT	VERIF_INSTITUTION

24

A3745453_24-000265

Pages 266 to / à 267

are withheld pursuant to sections

sont retenues en vertu des articles

s.16(1)(b), s.16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Pages 271 to / à 296

are withheld pursuant to sections

sont retenues en vertu des articles

s.16(1)(b), s.16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Watchtower

System Design

Advanced Analytics Solution Centre (A²SC)
November 2020

Immigration, Refugees
and Citizenship Canada

Immigration, Réfugiés
et Citoyenneté Canada

Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

AGENDA

Basic Operation

Data

    a) **Overview**

    b) **Inputs**

    c) **Adverse Targets**

    d) **Contextual Information**

System Configuration

ANNEX: System Design

Pages 299 to / à 301

are withheld pursuant to sections

sont retenues en vertu des articles

s.16(1)(b), s.16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Pages 305 to / à 307

are withheld pursuant to sections

sont retenues en vertu des articles

s.16(1)(b), s.16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Key Question for Project Team

{ **What role, if any, should governance play in these system design choices?** }

A3745462_12-000308

Pages 309 to / à 323

are withheld pursuant to sections

sont retenues en vertu des articles

s.16(1)(b), s.16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Page 324

is withheld pursuant to sections

est retenue en vertu des articles

16(1)(b), 16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Page 325

is withheld pursuant to sections

est retenue en vertu des articles

16(1)(b), 16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Page 326

is withheld pursuant to sections

est retenue en vertu des articles

16(1)(b), 16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Pages 327 to / à 329

are withheld pursuant to sections

sont retenues en vertu des articles

s.16(1)(b), s.16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Page 330

is withheld pursuant to sections

est retenue en vertu des articles

16(1)(b), 16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Page 333

is withheld pursuant to sections

est retenue en vertu des articles

16(1)(b), 16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

Meeting Instructions

1. CHAT FEATURE IN MS TEAMS

* Throughout this meeting, please post any questions, comments or considerations using the chat function in MS Teams as they arise during this meeting. These questions and comments will not be addressed directly in this session, but will be collected at the end of the meeting and used to frame subsequent project team discussions that will explore these issues in depth.

2. ROUNDTABLE (3 pm)

One participant from each team will be asked to:
1) introduce themselves
2) Identify their team's mandate as it relates to watchtower and
3) list one thing they would like to see achieved by the end of this project.

Watchtower

Process Design Project
Advanced Analytics Solution Centre (A2SC)
November 2020

Immigration, Refugees
and Citizenship Canada
Immigration, Réfugiés
et Citoyenneté Canada

Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

Project Goals

- Engage Key IRCC Stakeholders for deeper involvement and understanding on watchtower.

- Design, Draft and Test draft usage and governance processes for the tool.

- Lay key groundwork to support continued development of the tool at IRCC.

IN SCOPE
- Usage and governance
- Legal and privacy considerations
- Risk Identification/Mitigation

OUT OF SCOPE
- Technical design / development (user interface, etc.), with possible rare exceptions
- Areas covered by existing governance or operating procedures for risk assessment.

Immigration, Refugees
and Citizenship Canada

Immigration, Réfugiés
et Citoyenneté Canada

Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

Artefacts

Governance Framework
- Authorities, approvals, key decision-points, etc.

Usage Processes
- Documentation, officer instructions, retention, etc.

Legal & Privacy Opinions
- Possible updates to existing documents/drafts.

Project Risk Assessment / Mitigation Plan

Considerations Report
- "Parking Lot" for issues outside the scope of this project

Project Report

Immigration, Refugees   Immigration, Réfugiés
and Citizenship Canada   et Citoyenneté Canada
Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

Project Structure

Up to 12 weeks in length

Weekly project team meetings (1-hour)

Meetings will be a mix of:
- structured brainstorming sessions
- "in the weeds" working/design sessions; and
- presentations/demos

A2SC to act as convenor/facilitator

Non-administrative test run of watchtower will be used to frame project

Project Team: OPPB (A2SC), IRM, IPG, CN, DN, IN, Legal, Privacy, SPP, CMB, Admissibility

Watchtower

Risk Identification Tool

Advanced Analytics Solution Centre (A2SC)
November 2020

s.16(1)(b)

s.16(2)(c)

Watchtower

Pages 341 to / à 343

are withheld pursuant to sections

sont retenues en vertu des articles

s.16(1)(b), s.16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

DEMO

RoundTable

1) Introduce yourself (and any others participating from your team)

2) Identify your team's mandate as it relates to watchtower

3) One thing you would like to see achieved through this project

A2SC, IRM, IPG, CN, DN, IN, Legal, Privacy, SPP, CMB, Admissibility

Pages 346 to / à 355

are withheld pursuant to sections

sont retenues en vertu des articles

s.16(1)(b), s.16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information

# Privacy Needs Assessment for Watchtower Global SP Pilots

This document serves as a tool for the Department to assess the privacy needs for your initiative, document your program area's commitment to taking appropriate steps to protect privacy in your initiative, and to prioritize it in IRCC's privacy work plan. Based on this assessment, we may determine that no privacy work is required, or we may recommend:

- the development of a new Privacy Impact Assessment (PIA);
- an amendment or update to one or more existing PIAs or
- other privacy work, as appropriate.

It is essential that you provide accurate and complete information so that we can provide the most appropriate recommendations and optimal support.

Instructions and Responsibilities

Steps to complete the PNA Document

ACTION 1 – Program	ACTION 2 – ATIP	ACTION 3 – Program	ACTION 4 – ATIP
• Insert initiative name on **page 1** • Complete **Parts 1 & 2** • Notify ATIP *	• Complete **Part 3** • Notify Program	• Complete **Part 4** • Sign **Part 5** (Program Lead Director) • Notify ATIP *	• Sign **Part 5** - Chief Privacy Officer ** • Notify Program
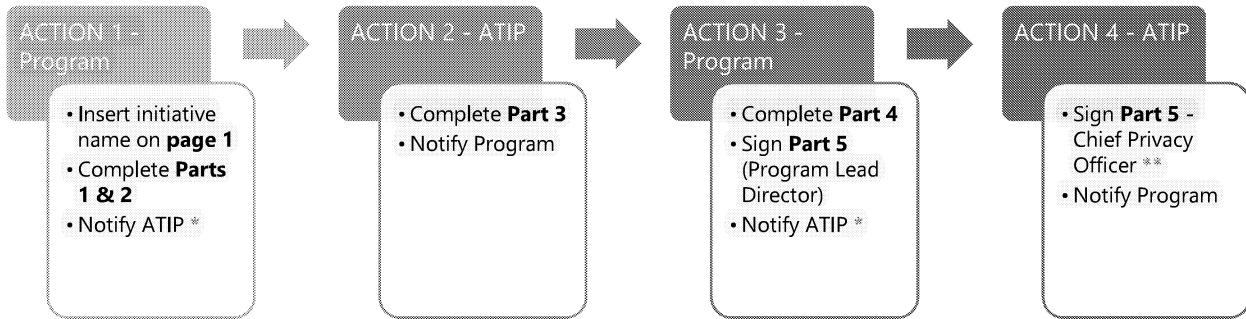
* Send the document to the ATIP Division.
** In cases where Privacy Compliance Evaluation (PCE) is being sought, you must obtain the signature of ADM Corporate Services Sector

Part 1 – General Information

The information provided in this section will be used to:

- better understand your initiative and how it aligns with departmental priorities; and
- prioritize our review and support of your initiative in a manner commensurate with its complexity and risk.

Initiative Business Owner

Sector/Branch/Division	IN, CN and DN
Director	Ellie Weber (CN)
Program area contact	Joshua Parkinson (CN)

Immigration, Refugees Immigration, Réfugiés
and Citizenship Canada et Citoyenneté Canada
Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

s.16(1)(b)

s.16(2)(c)

Description

Describe your initiative:

- What is the purpose? How will the initiative operate?
- How will the personal information be used? Specify whether personal information is being used to make decisions that directly affects individuals.
- Is this a new program or a modification to an existing one?
  - If it is a modification to an existing program, select from the options below, and be sure to describe both the existing program AND the proposed modifications

Does the initiative involve any of the following changes to current methods for handling personal information?

☐	Increased collection, use or disclosure	☐	Changing from paper-based to electronic	☐	Changing from manual to systematic disclosure
☐	New information sharing partners	☐	Increased or changed target population	■	New or enhanced technologies
☐	Changing from direct to indirect collection	☐	Enhanced investigation or surveillance	☐	Other

Alignment with IRCC's Departmental Results Framework

Identify all program activities in which the initiative is incorporated. If the information cannot be provided, only check the "Unsure" option at the bottom of the table below.

ATIP File #P20XXXX-XX

IRCC CORE RESPONSIBILITIES & PROGRAM ACTIVITIES (Check all applicable ones)

Visitors, International Students and Temporary Workers	Immigrant and Refugee Selection and Integration	Citizenship and Passports	Internal Services
☐ Visitors ■ International Students ☐ Temporary Workers	☐ Federal Economic Immigration ☐ Provincial Economic Immigration ☐ Family Reunification ☐ Humanitarian / Compassionate & Discretionary Immigration ☐ Refugee Resettlement ☐ Asylum ☐ Settlement	☐ Citizenship ☐ Passport	☐ Acquisition Services ☐ Communications Services ☐ Financial Management Services ☐ Human Resources Management Services ☐ Information Management Services ☐ Information Technology Services ☐ Legal Services ☐ Management & Oversight Services ☐ Material Services ☐ Real Property Services ☐ Travel & Other Administrative Services

☐ Unsure (*Provide a brief explanation*):

Alignment with Sector / IRCC / Government of Canada Priorities

Indicate if the initiative is linked to one or more sector, departmental or government of Canada priorities.

☐ No   ■ Yes ~ Describe the priority and provide links

> "Manage increased temporary resident volumes while advancing transformation", *IRCC 2018-2021 Integrated Plan*, p. 5

Timelines for Implementation

Provide the timeline for the initiative. Specify the start and end dates. If there is no end date, please specify whether the initiative is permanent, has no end date or the end date is unknown.

> Pilot will run for a limited time:

■ This initiative is a pilot project

COVID-19 Impact

Specify if the initiative is related to COVID-19. The Privacy Compliance Evaluation (PCE) is a streamlined way of conducting a privacy analysis for urgent COVID-related initiatives in lieu of a full PIA.

■ No   ☐ Yes (Provide a brief explanation below)

Immigration, Refugees   Immigration, Réfugiés
and Citizenship Canada   et Citoyenneté Canada
Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

ATIP File #P20XXXX-XX

☐   This COVID-related initiative continues beyond March 31, 2021.

If not, indicate the end date below.

Related Privacy Impact Assessments

To your knowledge, are there are any PIAs (completed or ongoing) related to this initiative or activity? If you are aware of PIAs related to similar initiatives at other federal departments, please include them as well.

☐   Unknown   ☐   No   ■   Yes

If yes, indicate below the titles of the other PIAs related to this one by specifying for each whether it is completed or still ongoing.

A2SC completed a PIA for its use of advanced analytics in support of TRVs from China and India (*"Privacy Impact Assessment: Use of Advanced Analytics in IRCC Programs"*). The work proposed here is very closely related.

Part 2 – Initial Privacy Considerations

Legal Authorities for Collection

The *Privacy Act* requires institutions to ensure there is **parliamentary authority** for the program or activity for which the personal information is collected, used and disclosed. Such authority is usually contained in:

- an Act of Parliament or subsequent Regulations;
- an approval of expenditures proposed in the Estimates and as authorized by an appropriation Act or;
- activities conducted as part of the administration of the program.

Identify the relevant authorities in the table below. We have included common legislative authorities at IRCC as examples.

Note: The *Privacy Act* is not a legislative authority for the collection or creation of personal information.

SOME COMMON LEGISLATIVE AUTHORITIES	SPECIFIC SECTION(S)
The Department of Citizenship and Immigration Act	
The Immigration and Refugee Protection Act	*186.1(1) and 186.1(5)*
The Immigration and Refugee Protection Regulations	
Citizenship Act	
Citizenship Regulations	
Canadian Passport Order	
Financial Administration Act **(for Internal Services)** *	
Insert other legislation if applicable...	

Immigration, Refugees   Immigration, Réfugiés
and Citizenship Canada   et Citoyenneté Canada
Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

ATIP File #P20XXXX-XX

* For internal service programs that draw authority from the *Financial Administration Act*, you must also specify which policies apply to the programs. Government of Canada policies can be found at: https://www.tbs-sct.gc.ca/pol/index-eng.aspx

Does this initiative require new legislation or an amendment to an existing piece of legislation?

■ No   ☐ Unknown   ☐ Yes (Please describe below)

Identifying a Personal Information Bank (PIB)

What is the Personal Information Bank (PIB) for your program or activity? Please select one of the options:

☐   Unknown

☐   A new PIB will need to be developed

■   There is an existing PIB. Please list the name and number below.

Two PIBs were updated to include computer analytics:
- Migration Control and Security Management (PPU 068)
- International Students (PPU 051)

Elements of Personal Information/Data Involved

From the non-exhaustive listing of possible data elements below, indicate all applicable data elements collected or created in the initiative by checking the box attached.

■   Not Applicable (no new collection of personal information)

Personal Information Categories			
☐	Contact information (name, phone number(s), mailing address, e-mail address)	☐	Passport information
☐	Physical attributes	☐	Biometric information (photo, fingerprint, etc.)
☐	Biographical	☐	Medical/health information
☐	Opinions or views	☐	Financial information
☐	Unique identifier (UCI, SIN, PRI) or equivalent number	☐	Employment information
☐	Immigration, Citizenship or Passport status	☐	Criminal information
☐	Immigration information	☐	National security history or information
☐	Citizenship information	☐	

If necessary, add below any other applicable data elements.

Partnerships

Other than the employees within the program area responsible for the initiative, indicate all <u>partners</u> involved in the handling of personal information/data throughout the life of this initiative and the <u>nature of their involvement</u>, whether fully or partially.

This includes other IRCC branches/divisions, other federal departments, municipal, provincial/territorial governments, foreign governments, foreign organizations, private organizations, etc.

☐   Not Applicable

PARTNERS	RESPONSIBILITIES (specify by adding an 'X' (copy/paste) at the corresponding one)				
	Collection	Access	Retention (storage)	Disposal	Other (specify)
A2SC		X	X	X	Analysis
IRM		X			Governance
Provide a brief description of how each responsibility is fulfilled: Identify MOUs or other similar instruments that currently govern the sharing or are under negotiation. IRM is currently drafting a governance and risk mitigation framework for Watchtower.					

Other Considerations

Indicate if the initiative involves any of the following:

■	Information belonging to another organization	☐	Data matching ~ personal information from one database is linked or combined with personal information from another database
☐	Publicly available information	☐	<u>Statutory Prohibitions</u>
☐	Cloud computing	■	Complex System Access or Storage*
☐	Chat bots	☐	Active or passive surveillance, monitoring or investigation
■	Analytics	☐	Audio or video recording for quality control
☐	Artificial intelligence	☐	Other
☐	Social media	☐	None of the above
☐	Web scraping ~ web data extraction		

* Information of partners is stored in a system where different parties have access, information of multiple programs are saved in the same system, or parties other than IRCC have been given or will be given access to a system containing IRCC information - GCMS meets all three criteria, as an example

If you check any of the above boxes, elaborate below.

s.16(1)(b)

s.16(2)(c)

Privacy Concerns

Is it anticipated that the public or departmental employees will have any privacy concerns regarding the proposed program or service?

☐ Yes (Please describe below)   ☐ No   ■ Unknown

Part 3 - ATIP Needs Assessment

Clarification is required before a recommendation can be made	☐ Yes	☐ No
A new or modified PIA is required	☐ Yes	☐ No
A new or modified privacy protocol is required	☐ Yes	☐ No
Limited privacy work is required	☐ Yes	☐ No
No privacy work is required at this time	☐ Yes	☐ No

ATIP Recommendation and Rationale

Part 4 - Program Decision

☐ We concur with the assessment and will follow the ATIP Division's recommendations.

-OR-

☐ We do not concur with the assessment and will not follow the ATIP Division's recommendations.

Describe what actions you will take instead of the ATIP Division recommendations.

-OR-

Immigration, Refugees
and Citizenship Canada
Immigration, Réfugiés
et Citoyenneté Canada

Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

ATIP File #P20XXXX-XX

In cases where a PIA is required, but the initiative is **COVID-related and the urgency** will prevent the department from submitting a PIA prior to implementation, the Treasury Board of Canada Secretariat (TBS) has issued an Interim Directive on Privacy Impact Assessment to address the challenges initiatives might deal with while complying with privacy law and rules. This Interim Directive (section 6.4) allows, **in exceptional circumstances**, the completion of a Privacy Compliance Evaluation (PCE) in lieu of a full PIA, as a streamlined way of conducting a privacy analysis for **urgent COVID-related initiatives**.

For COVID-related initiatives that end by March 31, 2021:
☐ Because of the urgency of the initiative, we are seeking approval from the ADM Corporate Services Sector to complete a PCE (in lieu of a PIA) prior to implementation.

For COVID-related initiatives that continue past March 31, 2021:
☐ Because of the urgency of the initiative, we are seeking approval from the ADM Corporate Services Sector to complete a PCE (in lieu of a PIA) prior to implementation. We commit to completing a PIA before September 30, 2021, in addition to the PCE.

Justification for the PCE

Explain the urgency of the initiative and demonstrate why a PIA cannot be completed prior to implementation.

Part 5 - Record of Sign-Off

Signature instructions

(1) Right-click on the signature block & select the option "Signature Setup…"
(2) Go to "Suggested signer": replace the current content with the complete name of the Program Director
(3) Go to "Suggested signer's title": replace "[Division Name]" with the official name of your Division
(4) Click on "OK"
(5) Right-click on the signature block & select the option "Sign"

X _____

[Program Lead Name]
Program Lead Director, [Division Name]

Immigration, Refugees   Immigration, Réfugiés
and Citizenship Canada   et Citoyenneté Canada
Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

ATIP File #P20XXXX-XX

X
_____

Simon Cardinal
Chief Privacy Officer

For Covid-related Initiatives

I authorize the program area to complete a PCE in lieu of a PIA (as identified in Part 4).

☐ Yes   ☐ No

X
_____

Holly Flowers Code
A/ADM, Corporate Services

s.16(1)(b)

s.16(2)(c)

Immigration, Refugees
and Citizenship Canada
Immigration, Réfugiés
et Citoyenneté Canada
Information disclosed under the Access to Information Act
L'information divulguée en vertu de la loi sur l'accès à l'information

Protected B

s.23

Document Change Control

Version#	Changed By	Date of Change	Description of Changes
1.0	Scott Wakeman	Jan 21, 2021	First Draft
2.0	Scott Wakeman	Feb 4, 2021	Adjustments based on feedback on first draft from IRM, Legal Services and Privacy
3.0	Scott Wakeman	Feb 26, 2021	including key risks identified and A2SC comments/proposed mitigations
4.0	Mike Haymes	Aug 13, 2021	Updated for the new pilot working group members, approval details added

Contents

Protected B

Project Approval

This project was approved for deployment on June 25, 2021, by the Director General of OPPB. This approval followed briefings on the project with the ADM, Operations, and presentation to the Data Executive Steering Committee (DESC) on June 1, 2021. The pilot was also endorsed by the Integrated Network Steering Committee (INSC) meeting on May 13, 2021.

Protected B

A3745474_13-000377

Page 378

is withheld pursuant to sections

est retenue en vertu des articles

16(1)(b), 16(2)(c)

of the Access to Information Act

de la Loi sur l'acces a l'information